BitDefender 8 Standard

Manuel d’utilisation

bitdefender
secure your every bit

Index

Accord de licence 4

Licence du logiciel **4**

Accord de licence **5**

Système de secours BitDefender 8

Configuration minimale **8**

Comment analyser **8**

Booter depuis le CD 8

Installer le pilote NTFS 9

Vérifiez votre disque dur 9

Sélectionner les options d'analyse 9

Commencer l'analyse 11

Installation 12

Système requis **12**

Etapes d'installation **12**

Supprimer, réparer ou modifier les fonctions de BitDefender 8 Standard **14**

Description du produit 15

Description **15**

Principales fonctions **15**

Antivirus 15

Mise à jour 16

Autres caractéristiques **16**

La console de contrôle 17

Vue d'ensemble **17**

Module Général **19**

Etat 19

Résident 19

Mise à jour automatique 20
Enregistrement du produit 20
Paramétrages de la console de contrôle 21
A propos 23
Module Antivirus.... 24
Analyse à l'accès 25
Contrôle des registres....25
Sélectionner les principaux paramétrages 27
Sélectionner d'autres options 27
Analyse à la demande 29
Analyse immédiate 29
Analyse programmée....37
Isoler les fichiers infectés 45
Afficher les fichiers rapports 47
Désinfection d'un virus détecté.... 48
Module Mise à jour 49
Mise à jour manuelle 50
Mise à jour automatique 51
Emplacement mises à jour 51
Options de mise à jour automatique....52
Options de l'interface....52

Meilleurs conseils 53
Antivirus 53

Questions courantes....54
Général 54
Antivirus 54
Mise à jour 55

Glossaire 56

Informations contact 61

1

Accord de licence

Licence du logiciel

Le package BitDefender est protégé par la loi du copyright et par les traités internationaux concernant le copyright aussi bien que par d'autres lois et traités concernant la propriété intellectuelle. La loi du copyright, aussi bien que d'autres lois de la propriété intellectuelle, protège dans beaucoup de pays les droits des propriétaires de logiciel, en leur accordant quelques droits exclusifs, comprenant le droit de reproduire et de copier le logiciel. La reproduction du logiciel sans la permission du propriétaire représente une "infraction de copyright" et la loi impose dans ce cas des pénalités et des punitions.

Le logiciel est considéré comme reproduit quand:

- Il est chargé dans la mémoire de votre ordinateur par l'intermédiaire du lecteur de disquettes, du disque dur, du CD-ROM, ou d'autres medias;
- Il est copié sur un autre support, tel que la disquette ou le disque dur;
- Il est exécuté sur l'ordinateur depuis un serveur de réseau où le logiciel est résident ou déposé.

A peu près tout logiciel commercial est directement ou indirectement autorisé par le détenteur de copyright---le producteur du logiciel---pour usage final, par l'intermédiaire d'un contrat de licence. Des logiciels différents peuvent avoir différents types de contrats de licenciement.

BitDefender est une marque déposée de SOFTWIN. Microsoft, Windows, Excel, Word et les logos de Windows, Windows NT et Windows 2000 sont des marques déposées de Microsoft Corporation. Toutes autres marques déposées sont la propriété de leurs propriétaires respectifs.

Accord de licence

SI VOUS N'ACCEPTEZ PAS CES TERMES ET CONDITIONS, N'INSTALLEZ PAS CE LOGICIEL.
EN CLIQUANT SUR " OUI " OU EN INSTALLANT ET UTILISANT CE LOGICIEL, VOUS INDIQUEZ AVOIR COMPRIS ET ACCEPTÉ LES TERMES DE CET ACCORD.

Cet accord de licence est un accord légal entre vous (entité individuelle ou utilisateur final) et SOFTWIN pour l'usage du produit de SOFTWIN identifié au-dessus, qui comprend le logiciel et qui peut comprendre les éléments média, les matériels imprimés et la documentation " en ligne " ou électronique (" BitDefender "), le tout étant protégé par la loi française et par les lois et les traités internationaux. En installant, copiant, ou utilisant de toute autre manière le logiciel BitDefender, vous acceptez les termes de cet accord. Si vous n'agréez pas les termes de cet accord, n'installez pas et n'utilisez pas BitDefender.

BitDefender est protégé par les lois du copyright et par les traités internationaux concernant le copyright, ainsi que par les autres lois et traités concernant la propriété intellectuelle. BitDefender est licencié et non pas vendu.

Droits de licence Ce logiciel restant la propriété de SOFTWIN, vous disposez néanmoins de certains droits d'utilisation une fois l'accord de licence accepté. Vos droits et obligations relatifs à l'utilisation de ce logiciel sont les suivants:

LOGICIEL. Vous pouvez installer et utiliser une seule copie de BitDefender ou de toute version antérieure sur le même système d'exploitation, sur un seul poste de travail. L'utilisateur principal de l'ordinateur, sur lequel BitDefender est installé, peut faire une copie additionnelle (seconde) pour son usage exclusif ou pour l'usage sur un ordinateur portable.

USAGE EN RÉSEAU. Vous pouvez emmagasiner ou installer une copie de BitDefender sur un dispositif de stockage, comme le serveur de réseau, employé seulement pour installer ou exécuter sur les autres ordinateurs d'un réseau interne ; néanmoins, vous devez acheter et dédier une licence séparée pour chaque terminal d'ordinateur sur lequel BitDefender est installé ou exécuté depuis le dispositif de stockage. Une licence de BitDefender ne peut pas être partagée ou utilisée de manière concurrentielle sur des postes ou terminaux d'ordinateurs multiples. Vous devrez acheter un pack de licences si vous en envisagez l'usage sur différents ordinateurs.

PACK DE LICENCES. Si vous achetez un Pack de Licences et que vous ayez acquis cet Accord de licence pour plusieurs licences de BitDefender, vous pouvez réaliser le nombre de copies du logiciel spécifié au-dessus comme "Copies licenciées". Vous avez aussi le droit de réaliser un nombre correspondant de copies pour l'usage sur des ordinateurs portables, comme spécifié ci-dessus dans la section "LOGICIEL".

TERMES DE LA LICENCE. La licence accordée ci-dessus commencera au moment où vous installez, copiez ou utilisez de toute autre manière BitDefender pour la première fois et continuera seulement pour l'ordinateur sur lequel le logiciel a été premièrement installé.

MISES À JOUR. Si BitDefender constitue une mise à jour, vous devez être correctement licencié pour utiliser le produit identifié par SOFTWIN comme étant éligible pour la mise à jour, afin d'utiliser BitDefender. Un produit BitDefender qui constitue une mise à jour remplace le produit qui formait la base de votre éligibilité pour

la mise à jour. Vous pouvez utiliser le produit résultant seulement en accord avec les termes de cet Accord de licence. Si BitDefender est une mise à jour d'un composant d'un progiciel que vous avez acheté comme un seul produit, BitDefender peut être utilisé et transféré seulement comme une partie de ce progiciel et ne peut pas être séparé pour l'usage sur plus d'un ordinateur.

COPYRIGHT. Tous les droits d'auteur de BitDefender (comprenant mais ne se limitant pas à toutes les images, photographies, logos, animations, vidéo, audio, musique, texte et " applets " compris dans BitDefender), les matériels imprimés qui l'accompagnent et les copies de BitDefender sont la propriété de SOFTWIN. BitDefender est protégé par les lois concernant le copyright et par les traités internationaux. C'est pourquoi vous devez traiter BitDefender comme tout autre matériel protégé par le copyright à l'exception du fait que vous pouvez installer BitDefender sur un seul ordinateur, vu que vous gardez l'original seulement pour archive. Vous ne pouvez pas copier les matériels imprimés qui accompagnent BitDefender. Vous devez produire et inclure toutes les notices de copyright dans leur forme originale pour toutes les copies respectives du média ou de la forme dans laquelle BitDefender existe. Vous ne pouvez pas céder la licence, louer sous quelque forme que ce soit tout ou partie du logiciel BitDefender. Vous ne pouvez pas décompiler, désassembler, modifier, traduire ou tenter de découvrir le code source de ce logiciel ou créer des outils dérivés de BitDefender.

GARANTIE LIMITÉE. SOFTWIN garantit que le support sur lequel le logiciel est distribué est exempt de vices de matériaux et de fabrication pendant une période de trente (30) jours à compter de la date de livraison du logiciel. Votre seul recours en cas de manquement à cette garantie sera le remplacement par SOFTWIN du support défaillant durant la période de trente (30) jours à compter de la date de livraison du logiciel. SOFTWIN ne garantit pas que le logiciel répondra à vos besoins ni qu'il fonctionnera sans interruption ou sans erreur.

SOFTWIN REFUSE TOUTE AUTRE GARANTIE POUR BITDEFENDER, QUELLE SOIT EXPRESSE OU IMPLICITE. LA GARANTIE CI-DESSUS EST EXCLUSIVE ET REMPLACE TOUTES AUTRES GARANTIES, QU'ELLES SOIENT IMPLICITES OU EXPLICITES, Y COMPRIS LES GARANTIES IMPLICITES DE COMMERCIALISATION ET D'APPLICATION PARTICULIÈRE.

REFUS DES DOMMAGES. Toute personne qui utilise, teste ou évalue BitDefender admet les risques concernant la qualité et la performance de BitDefender. En aucun cas SOFTWIN ne sera tenu responsable à votre égard de tous dommages particuliers ou indirects, réclamations et pertes quelconques découlant de l'utilisation ou de l'incapacité d'utiliser le logiciel même si SOFTWIN a été avisé de l'éventualité de tels dommages.

NOTICE IMPORTANTE POUR LES UTILISATEURS. CE LOGICIEL N'EST PAS DÉSIGNÉ POUR DES MILIEUX DANGEREUX, DEMANDANT DES OPÉRATIONS OU UNE PERFORMANCE SANS ERREUR. CE LOGICIEL N'EST PAS RECOMMANDÉ DANS LES OPÉRATIONS DE NAVIGATION AÉRIENNE, INSTALLATIONS NUCLÉAIRES OU DES SYSTÈMES DE COMMUNICATION, SYSTÈMES D'ARMEMENT, SYSTÈMES ASSURANT DIRECTEMENT OU INDIRECTEMENT LE SUPPORT VITAL, CONTROLE DU TRAFFIC AÉRIEN, OU TOUTE AUTRE APPLICATION OU INSTALLATION OU LA DÉFAILLANCE POURRAIT AVOIR COMME EFFET LA MORT DES PERSONNES, DES BLESSURES PHYSIQUES SÉVÈRES OU DES DOMMAGES DE LA PROPRIÉTÉ.

RESTRICTIONS DE DROIT DU GOUVERNEMENT. Usage, duplication ou divulgation par le Gouvernement de BitDefender constituent sujet des restrictions stipulées par le sous paragraphe (c) (1) (ii) des Droits des Données Techniques et Software, clause DFARS 252.227-7013 ou sous paragraphes (c) (1) et (2) du Droit Commercial regardant le Software, clause 48 CFR 52.227-19. Contactez SOFTWIN au numéro 5,

rue Fabrica de Glucoza, 72 322 - Sect. 2, Bucarest, Roumanie ou au Tél. 40-21-2330780 ou Fax : 40-21-2330763.

CONDITIONS GÉNÉRALES. Cet accord est régi par les lois de la Roumanie et par les règlements et les traités internationaux concernant le copyright. Cet Accord peut être modifié par une annexe de licence qui accompagne cet Accord ou par un document écrit qui ait été signé par vous et par SOFTWIN. Les prix, les coûts et les frais d'usage de BitDefender peuvent changer sans que vous en soyez prévenu. Dans l'éventualité d'une invalidité de tout règlement de cet Accord, cette invalidité n'affectera pas la validité du reste de cet Accord. BitDefender et le logo de BitDefender sont des marques déposées de SOFTWIN. Microsoft, Windows, Excel, Word, le logo de Windows, Windows NT, Windows 2000 sont des marques déposées de la Corporation Microsoft. Toutes les autres marques appartiennent à leurs propriétaires respectifs.

2

Système de secours BitDefender

BitDefender 8 Standard est équipé d'un CD bootable (**Système de secours BitDefender** basé sur **LinuxDefender**) qui est capable d'analyser et désinfecter tous les disques durs existants avant le démarrage de votre système d'exploitation.

Vous devriez utiliser le **Système de secours BitDefender** quand votre système d'exploitation ne fonctionne pas correctement à cause d'une infection virale. Cela survient d'habitude quand vous n'utilisez pas de produit antivirus.

La mise à jour des définitions des virus est automatique, sans l'intervention de l'utilisateur à chaque fois que vous lancez **Système de secours BitDefender**.

Configuration minimale

- Processeur compatible Intel (Pentium 200/300MHz ou +);
- 64 Mo de mémoire RAM pour le mode texte, minimum 256Mo pour le mode graphique avec KDE (512 Mo recommandés);
- Carte graphique compatible standard SVGA.

Comment analyser

Etapes à suivre afin d'analyser votre ordinateur contre les virus:

Booter depuis le CD

Insérez le **Disque de secours BitDefender** dans votre lecteur CD et redémarrez votre ordinateur.

Cela va lancer de manière automatique **Système de secours BitDefender** (éventuellement vous devez configurer le BIOS de votre ordinateur pour booter depuis le CD).

L'interface graphique **Système de secours BitDefender** apparaîtra:

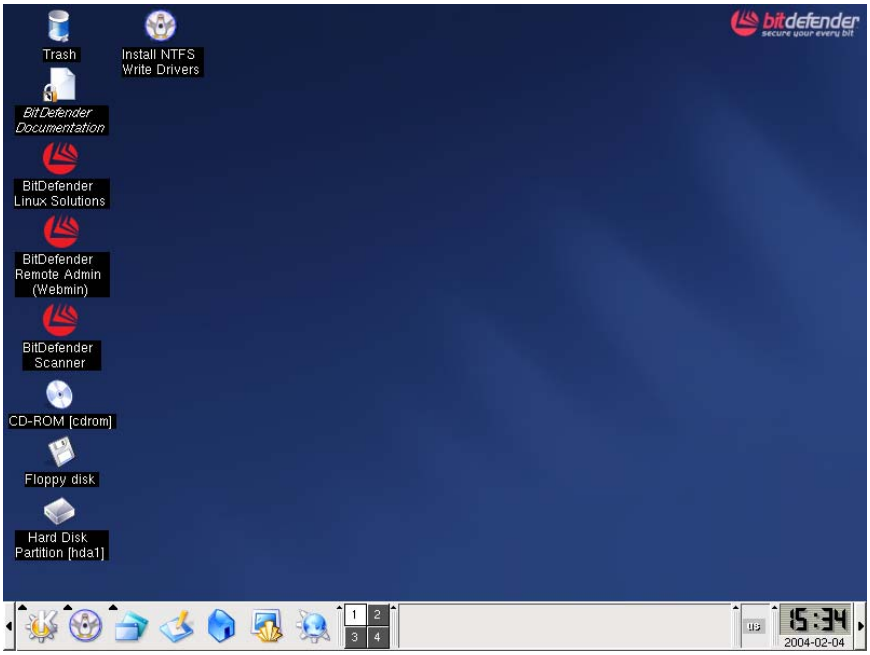


Figure 1

Installer le pilote NTFS

Cliquez sur l'icône **Install NTFS Write Drivers** avec la souris. Dans la fenêtre qui apparaîtra, cliquez deux fois sur **Forward**. Cela va lancer l'installation du logiciel NTFS. **LinuxDefender** a besoin de deux pilotes (`ntoskrnl.exe` et `ntfs.sys`) afin de pouvoir accéder à votre disque dur. Pour le moment, seulement les pilotes Windows XP sont supportés. Sachez que vous pouvez les utiliser pour accéder aussi aux partitions Windows 2000/NT/2003.

Pendant le processus d'installation vous allez recevoir le message suivant:

`Cannot open target file "/var/lib/capative/ext2fsd.sys": Read-only file System`.

Confirmez avec **OK**. Finalement cliquez sur **OK** pour fermer le processus d'installation.

Vous allez recevoir le message: `Although essential modules ...`. Cliquez sur **OK**.

Vérifiez votre disque dur

Sur le bureau **LinuxDefender** cliquez sur l'icône **Hard Disk Partition [hda1]**. Cela va ouvrir une fenêtre qui vous permettra de voir le contenu de votre disque dur. Fermez cette fenêtre.

Sélectionner les options d'analyse

Cliquez sur l'icône **BitDefender Scanner** afin de sélectionner les options d'analyse. La fenêtre suivante apparaîtra:

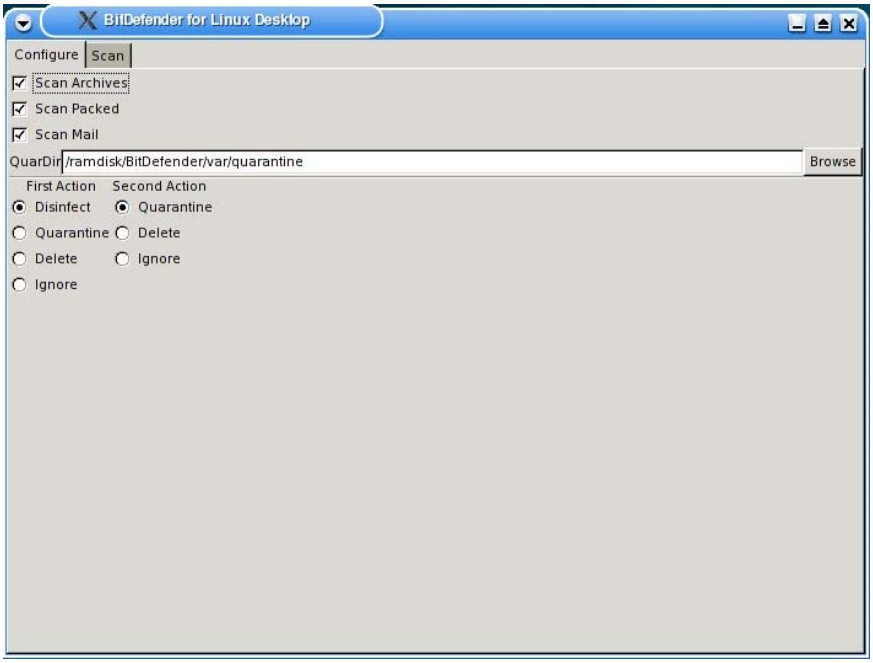


Figure 2

Les options suivantes sont disponibles:

- **Scan Archives** - analyse à l'intérieur des archives;
- **Scan Packed** – analyse les paquets des programmes;
- **Scan Mail** - analyse les bases de données de messagerie;
- **QuarDir** – le chemin par défaut vers le dossier de quarantaine est: `/ramdisk/BitDefender/var/quarantine`.

Si vous désirez changer le dossier de quarantaine cliquez sur **Browse** et sélectionner une location différente (ou vous pouvez la taper dans le champ **QuarDir**).

BitDefender essaie d'appliquer une action si un fichier infecté est trouvé. Vous pouvez donc choisir quelle action vous desirez. Si la première ne peut pas être appliquée, une deuxième (configurable aussi) le sera.

Astuce: Nous recommandons comme première action: **Disinfect**, et comme deuxième: **Delete**.

BitDefender permet la sélection de deux actions au cas ou un fichier infecté est trouvé. Vous pouvez sélectionner une des actions suivantes:

Première action	Description
Disinfect	Pour désinfecter le fichier infecté.
Quarantine	Les fichiers infectés sont déplacés dans la quarantaine. Au moment ou vous quittez **LinuxDefender**, le fichier de quarantaine sera effacé.
Delete	Efface les fichiers infectés immédiatement, sans aucun préavis.
Ignore	Au cas ou un fichier infecté sera trouvé, il sera ignoré.

Deuxième action	Description
Quarantine	Les fichiers infectés sont déplacés dans la quarantaine.
Delete	Efface les fichiers infectés immédiatement, sans aucun préavis.
Ignore	Au cas ou un fichier infecté sera trouvé, il sera ignoré.

Commencer l’analyse

Cliquez sur l’onglet **Scan**.

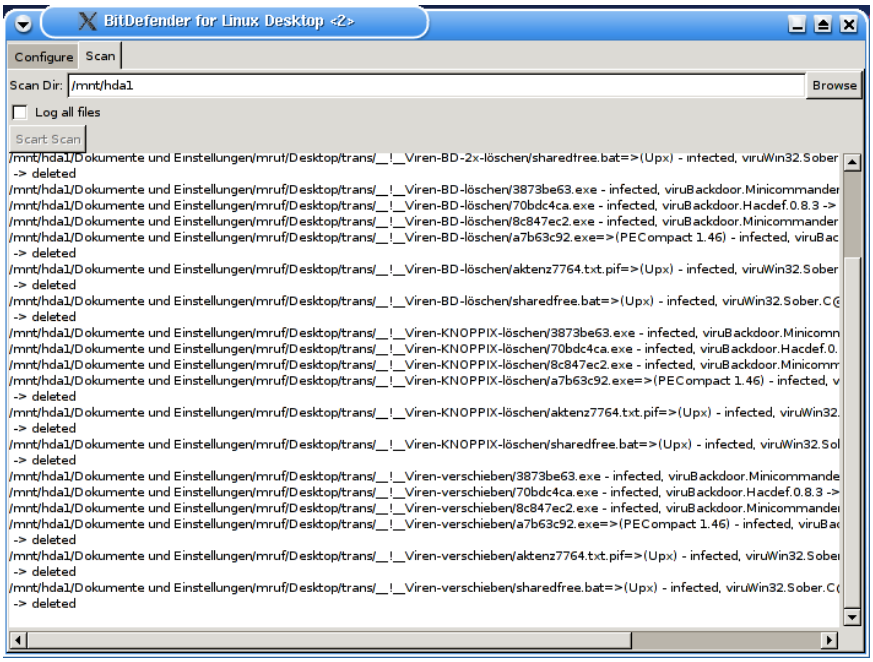


Figure 3

Dans le champ **Scan Dir** vous devez spécifier le chemin vers le disque dur comme suit.

Exemples:

Si vous avez un disque dur avec trois partitions, vous devez analyser chaque partition séparément.

- `/mnt/hda1` – pour la première partition;
- `/mnt/hda2` – pour la deuxième partition;
- `/mnt/hda3` – pour la troisième partition.

Si vous avez un deuxième disque avec deux partitions, la syntaxe est la suivante:

- `/mnt/hdb1`– pour la première partition;
- `/mnt/hdb2`– pour la deuxième partition.

Si vous utilisez un disque dur SCSI avec deux partitions, la syntaxe est la suivante:

- `/mnt/sda1`– pour la première partition;
- `/mnt/sda2`– pour la deuxième partition.

L’option **Log all files** est par défaut décochée car la vitesse d’analyse sera fortement diminuée avec cette option cochée.

Cliquez **Start Scan**. Cela va lancer l’analyse du disque dur.

Au moment ou un virus est trouvé, BitDefender vous en informera dans la fenêtre principale.

Note

Effectuez l’analyse contre les virus deux fois. Il est possible que le virus ne soit pas effacé la première fois que vous lancez l’analyse d’une partition NTFS.

3

Installation

Système requis

Pour assurer un fonctionnement correct du produit, vérifiez avant l'installation que vous disposez de la configuration suivante:

Processeur minimum : Pentium 200MHz ou compatible ;
Espace disque minimum : 40 Mo ;
Mémoire vive minimale : 64MB (128 Mo recommandés) ;
Système d'exploitation : Windows 98/NT-SP6/ME/2000/XP; Internet Explorer 4.0 (+).

Etapes d'installation

Introduisez votre CD dans le lecteur. Un écran d'accueil vous proposera d'installer BitDefender. Cliquez sur cette option.
Si vous avez acheté le produit par téléchargement, localisez le fichier d'installation et double-cliquez dessus avec la souris.
Dans les deux cas, cela lancera l'assistant d'installation, qui vous guidera à travers le processus d'installation.

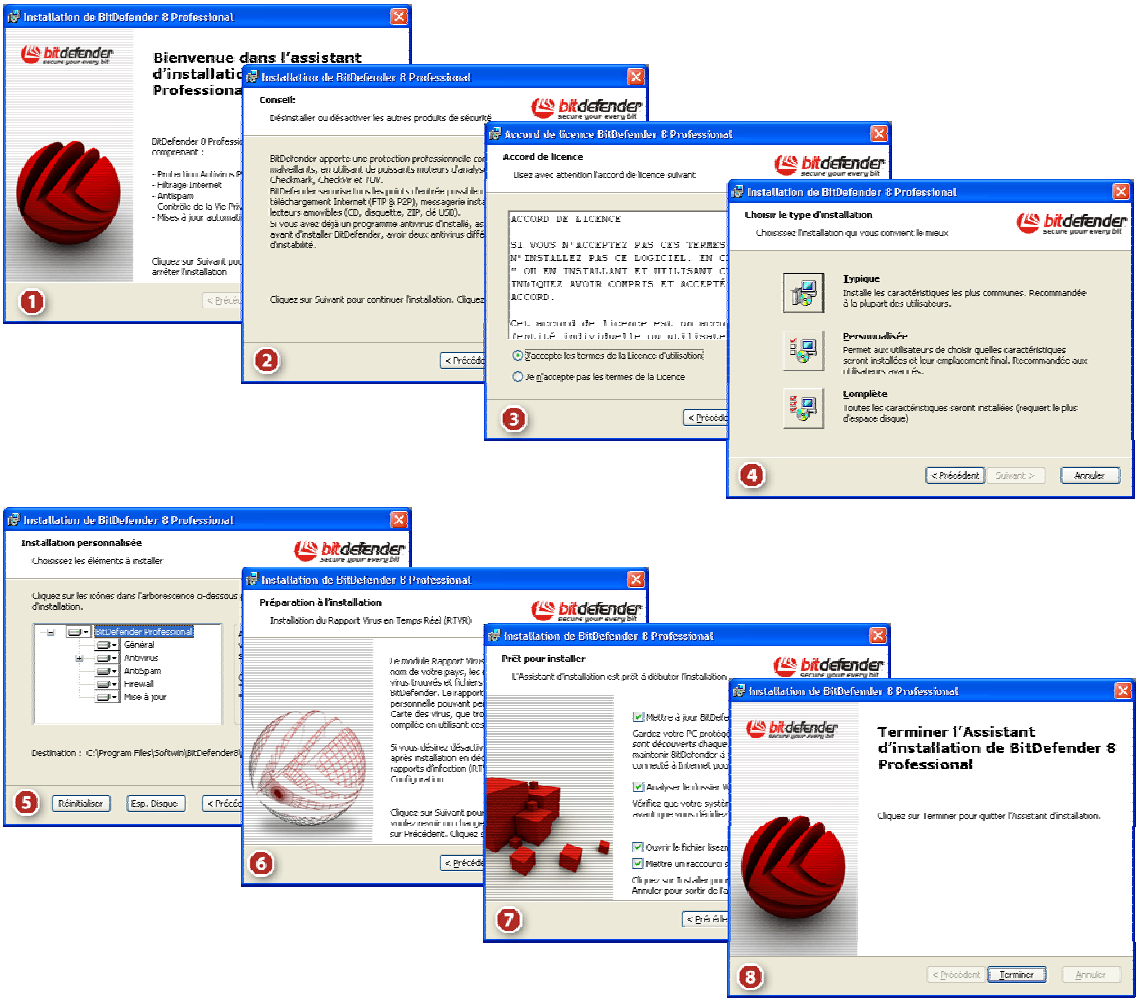

Installation de BitDefender 8 Professional
Bienvenue dans l'assistant d'installation de BitDefender 8 Professional
Cliquez sur Suivant pour continuer l'installation ou sur Annuler pour arrêter l'installation
Conseil:
Désinstaller ou désactiver les autres produits de sécurité
Cliquez sur Suivant pour continuer l'installation. Cliquez sur Précédent pour revenir à la page précédente.
Accord de licence
Lisez avec attention l'accord de licence suivant:
ACCORD DE LICENCE
J'accepte les termes de la licence d'utilisation
Je n'accepte pas les termes de la licence
Choisir le type d'installation
Choisissez l'installation qui vous convient le mieux
Typique
Installe les caractéristiques les plus communes. Recommandée à la plupart des utilisateurs.
Personnalisée
Permet aux utilisateurs de choisir quelles caractéristiques seront installées et leur emplacement final. Recommandée aux utilisateurs avancés.
Complète
Toutes les caractéristiques seront installées (requiert le plus d'espace disque)
Précédent
Suivant >
Annuler
Installation personnalisée
Choisissez les éléments à installer
Cliquez sur les icônes dans l'arborescence ci-dessous pour modifier la façon dont les éléments seront installés.
BitDefender Professional
Général
Antivirus
Antispam
Firewall
Mise à jour
Destination : C:\Program Files\Software\BitDefender8\
Réinitialiser
Esp. Disque
Préparation à l'installation
Installation du Rapport Virus en Temps Réel (RTVR)
Prêt pour installer
L'Assistant d'installation est prêt à débuter l'installation.
Mettre à jour BitDefender
Ouvrir le fichier lisez-moi
Mettre un raccourci sur le bureau
Terminer l'Assistant d'installation de BitDefender 8 Professional
Cliquez sur Terminer pour quitter l'Assistant d'installation.
Terminer
1
2
3
4
5
6
7
8

Figure 4

Etapes d'installation:

1. Cliquez sur **Suivant** pour continuer ou sur **Annuler** si vous voulez quitter l'installation.
2. Cliquer sur **Suivant** pour continuer ou sur **Retour** pour revenir à la première étape.
3. Merci de lire l' **Accord de Licence**, sélectionnez **J'accepte les termes de l'Accord de Licence** et cliquez sur **Suivant**. Si vous n'acceptez pas ces conditions, sélectionnez **Je n'accepte pas les termes de l'Accord de Licence** et cliquez sur **Annuler**. Le processus d'installation sera abandonné et vous sortirez de l'installation.
4. Vous pouvez choisir quel type d'installation vous souhaitez : typique, personnalisée ou complète.

   - **Typique** – Le programme sera installé avec les options les plus communes. Cela est recommandé pour la plupart des utilisateurs.
   - **Personnalisée** – Cela vous donne la possibilité de choisir les composants que vous souhaitez installer. Recommandé pour les utilisateurs « avancés » uniquement.
   - **Complète** – Pour l'installation complète du produit. L'ensemble des modules BitDefender seront installés.

   Si vous choisissez **typique** ou **complète** vous ne passerez pas par l'étape 5.

5. Si vous avez sélectionné **Personnalisé** une nouvelle fenêtre apparaîtra, contenant la liste de tous les composants de BitDefender afin de pouvoir choisir ceux que vous souhaitez installer.

Si vous cliquez sur l'un des composants, une courte description (incluant l'espace disque nécessaire) s'affichera sur le côté droit. Si vous cliquez sur un menu apparaîtra avec la possibilité de choisir d'installer ou non le module sélectionné.

Vous pouvez sélectionner le répertoire dans lequel installer le produit. Le répertoire par défaut est `C:\Program Files\Softwin\BitDefender 8`.

Si vous voulez choisir un autre répertoire, cliquez sur **Parcourir** et, dans la fenêtre qui s'ouvre, choisissez le répertoire. Cliquer sur **Suivant**.

6. Cliquez sur **Suivant**.
7. Vous avez quatre options sélectionnés par défaut:
   - ➔ **Mise à jour BitDefender** – pour mettre à jour BitDefender à la fin de l'installation. Votre système doit être connecté à Internet pour cela.
   - ➔ **Lancer une analyse complète du système** – pour rechercher des virus sur le PC à la fin de l'installation.
   - ➔ **Ouvrir le fichier lisezmoi** – pour ouvrir le fichier lisezmoi à la fin de l'installation.
   - ➔ **Créer un raccourci sur le bureau** – pour mettre un raccourci sur le bureau à la fin de l'installation.

   Cliquez sur **Installer** afin de commencer l'installation du produit.
8. Cliquez sur **Terminer** pour compléter l'installation du produit. Si vous avez accepté les paramétrages par défaut pour le répertoire d'installation, un nouveau répertoire du nom de **Softwin** est créé dans **Program Files**, contenant un sous-répertoire **BitDefender 8**.

Note
Il vous sera peut être demandé de redémarrer votre système pour terminer le processus d'installation.

Supprimer, réparer ou modifier les fonctions de BitDefender 8 Standard

Si vous voulez modifier, réparer ou supprimer **BitDefender 8 Standard**, suivez le chemin depuis le menu Démarrer de Windows: **Démarrer → Programmes → BitDefender 8 → Modifier, reparer ou desinstaller**.

Il vous sera demandé confirmation de votre choix en cliquant sur **Suivant**. Une nouvelle fenêtre apparaîtra dans laquelle vous pourrez choisir:

- **Modifier** – pour sélectionner de nouveaux composants du programme à ajouter ou pour sélectionner des composants déjà installés et à retirer.
- **Réparer** – pour réinstaller tous les composants choisis lors de l'installation précédente.
- **Supprimer** – pour supprimer tous les composants installés.

Pour continue le processus, sélectionnez l'une des trois options listées ci-dessus. Nous recommandons **Supprimer** pour refaire une installation. Après la désinstallation, supprimez le sous-répertoire **Softwin** dans le répertoire **Program Files** pour assurer une nouvelle installation propre.

4

Description du produit

Description

Un bon logiciel antivirus ne suffit plus malheureusement tout seul dans un réseau. Les menaces informatiques ne proviennent pas seulement des virus, mais aussi des individus tels les hackers. L'équipe de développement BitDefender reconnaît que le milieu informatique présent comporte beaucoup de risques, c'est pourquoi elle vient de créer un paquet de logiciels de sécurité.

BitDefender 8 Standard intègre des modules antivirus et mise à jour dans un paquet de logiciels de sécurité, spécialement conçu pour les besoins des utilisateurs Internet, individuels ou entreprises.

Principales fonctions

BitDefender 8 Standard inclut 2 modules de protection: **Antivirus** et **Mise à jour**.

Antivirus

La mission du module AntiVirus est d'assurer la détéction et la désinfection de tous les virus en liberté. BitDefender Antivirus utilise des moteurs avancés d'analyse, certifiés par **ICSA Labs**, **Virus Bulletin, Checkmark, Checkvir** et **TUV**.

Protection Antivirus permanente

Les nouveaux moteurs d'analyse de BitDefender analysent et désinfectent les fichiers à l'accès, minimisant les pertes des données. Les documents infectés peuvent maintenant être récupérés au lieu d'être effacés.

Protection des applications de messagerie instantanée

Vous protège contre les virus qui se propagent par la messagerie instantanée et les logiciels de partage de fichiers.

Blocage comportemental innovant

Bloque les applications malicieuses suivant leur comportement. Cette méthode assure une protection proactive contre les nouveaux virus, chevaux de Troie, vers Internet et autres codes malicieux. Le système des fichiers, les registres et l'activité Internet sont constamment surveillés.

Quarantaine et rapports
Les fichiers suspicieux/infectés peuvent être aussi archivés dans une zone de quarantaine avant d'être désinfectés ou effacés. Le contenu de la quarantaine peut être envoyé aux laboratoires BitDefender, pour une analyse plus détaillée. Les fichiers non-infectés peuvent être remis facilement à leur place initiale.

Protection complète de la messagerie
L'application fonctionne au niveau du protocole POP3, bloquant tout message infecté, quel que soit le client de messagerie utilisé (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Lotus Notes, Pegasus, The Bat, etc), sans aucune configuration supplémentaire.

Mise à jour

Celui-ci est le module qui effectue la mise à jour du produit avec de nouvelles signatures virales et nouvelles options.

Mises à jour rapides, gratuites et automatiques
Mise à jour intelligente de la protection antivirus, ne nécessitant pas l'intervention de l'utilisateur. La mise à jour peut être faite à partir du réseau, directement de l'Internet ou par un serveur proxy. Les possesseurs des licences BitDefender bénéficient des mises à jour gratuites des définitions virales et du produit.

Auto-réparation
Le produit est capable de se réparer tout seul si nécessaire, en téléchargeant les fichiers endommagés ou manquants à partir des serveurs de BitDefender.

Mise à jour automatique
Les mises à jour de l'antivirus sont gratuites et automatiques. Les vérifications pour les nouvelles mises à jour peuvent être programmées aussi souvent que nécessaire.

Autres caractéristiques

Aide à la décision
Les assistants de configuration vous guideront à travers les étapes à suivre pour sécuriser votre système. Enfin, BitDefender vous informera directement sur votre bureau, dans une fenêtre discrète, de différentes alertes sur l'état de votre produit (mise à jour, date de dernière analyse…).

Facile à installer et à utiliser
Un assistant extrêmement intuitif vous guide à travers le processus d'installation. Une interface simple et amicale vous facilite l'utilisation du produit.

Support technique professionnel 24/24 – 7/7
Assuré par des personnes compétentes et une base de données en ligne qui répond aux questions les plus fréquemment posées.

5

La console de contrôle

Vue d'ensemble

BitDefender 8 Standard a été conçu avec une console de management (gestion) centralisée, qui permet la configuration des options de protection de chaque module BitDefender. Autrement dit, il suffit d'ouvrir la console pour accéder aux différents modules : **Antivirus** et **Mise à jour**.

L'accès à cette console se fait par le menu Démarrer de Windows, en suivant le chemin suivant: **Démarrer → Programmes → BitDefender 8 → BitDefender 8 Standard** ou plus rapidement en double-cliquant sur l'icône BitDefender dans la zone de notification (en bas à droite à côté de l'horloge).

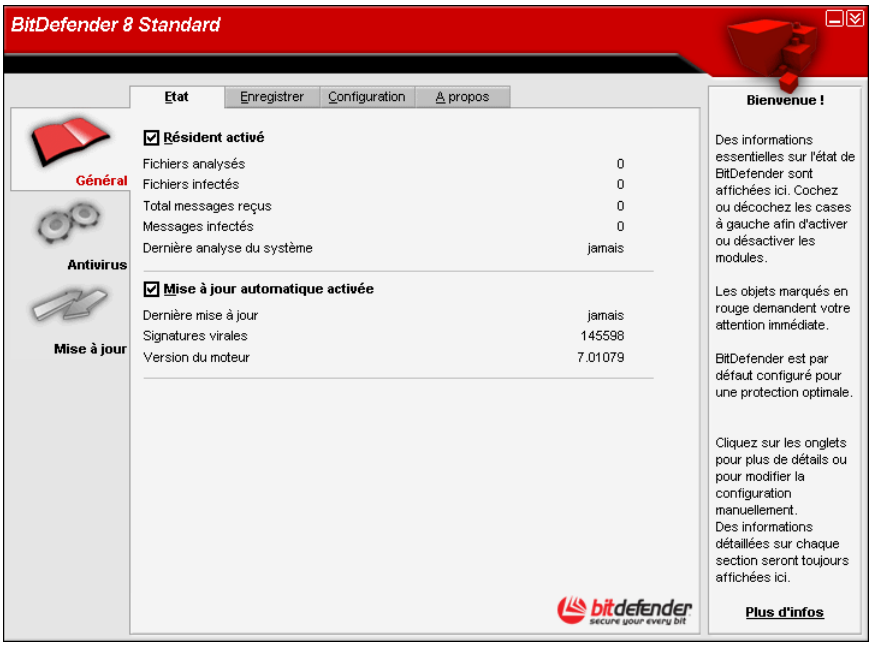

BitDefender 8 Standard
Etat
Enregistrer
Configuration
A propos
Général
Antivirus
Mise à jour
Résident activé
Fichiers analysés 0
Fichiers infectés 0
Total messages reçus 0
Messages infectés 0
Dernière analyse du système jamais
Mise à jour automatique activée
Dernière mise à jour jamais
Signatures virales 145598
Version du moteur 7.01079
bitdefender
secure your every bit
Bienvenue !
Des informations essentielles sur l'état de BitDefender sont affichées ici. Cochez ou décochez les cases à gauche afin d'activer ou désactiver les modules.
Les objets marqués en rouge demandent votre attention immédiate.
BitDefender est par défaut configuré pour une protection optimale.
Cliquez sur les onglets pour plus de détails ou pour modifier la configuration manuellement.
Des informations détaillées sur chaque section seront toujours affichées ici.
Plus d'infos

Figure 5

Sur la partie gauche de la console, vous pouvez sélectionner les modules suivants:

- Général – pour accéder à la section résumant les principaux paramétrages de BitDefender, des informations produits et contacts. Vous pouvez également enregistrer le produit à cet endroit.
- Antivirus – pour accéder à la fenêtre de configuration de l'antivirus.
- Mise à jour – pour accéder à la fenêtre de configuration des mises à jour.

L'option **Plus d'infos**, placée en bas à droite ouvre la section **Aide**.

Lorsque la console est réduite, une icône apparaît dans le zone de notification.

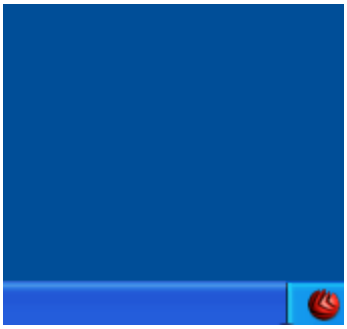


Figure 6

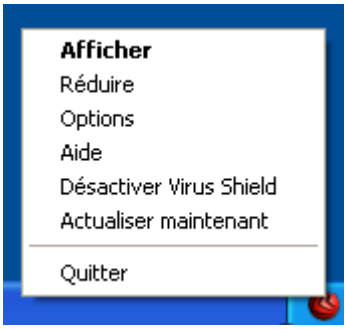


Figure 7

Si vous double-cliquez sur cette icône, la console s'ouvre.

De plus, en faisant un clic-droit dessus, comme dans la *Figure 7*, un menu contenant les options suivantes, apparaîtra.

- **Afficher** - ouvre la console de contrôle.
- **Réduire** - minimise la console, si elle est ouverte.
- **Options** - ouvre une fenêtre avec les options de la console.
- **Aide** - ouvre la documentation électronique.
- **Activer / Désactiver Virus Shield** – active / désactive Virus Shield.
- **Actualiser maintenant** – réalise une mise à jour immédiate.
- **Quitter** – ferme l'application. En choisissant cette option, l'icône dans la zone de notification disparaîtra. Pour la faire apparaître de nouveau, vous devrez la lancer depuis le menu **Démarrer**.

Note

Si vous désactivez une ou plusieurs des modules BitDefender, l'icône sera grisée. Ainsi vous saurez si quelques modules sont désactivés sans ouvrir la console de gestion.
L'icône va clignoter si une mise à jour est disponible.

Barre d'analyse d'activité

Certains d'entre vous ont certainement été surpris par le "petit rectangle gris" qui peut être déplacé sur l'écran.

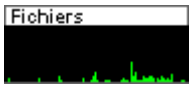


Figure 8

Cette fenêtre est une visualisation graphique de l'analyse d'activité de votre système.

Les barres vertes (la **Zone de fichiers**) montrent le nombre de fichiers analysés par seconde, sur une échelle de 0 à 50.

Note

La **Barre de l'activité d'analyse** vous annonce si le **Virus Shield** est désactivé avec une croix rouge sur l'aire **Zone Fichier**. Ainsi vous saurez si vous êtes protégé sans ouvrir la console de gestion.

Si vous ne souhaitez plus voir cette barre, il vous suffit de faire un clic-droit dessus et de choisir **Cacher**.

Astuce: Pour cacher complètement cette fenêtre, décochez l'option **Afficher la barre d'analyse d'activité** (depuis le module **Antivirus**, section Résident).

Module Général

BitDefender est par défaut paramétré pour une sécurité optimale. Les informations essentielles sur les modules de BitDefender sont affichées dans le module **Général**.

Il contient 4 sections différentes: Etat, Enregistrer, Configuration et A propos.

Etat

Vous pouvez consulter ici les informations concernant les status du produit.

BitDefender 8 Standard
Etat
Enregistrer
Configuration
A propos
Général
Antivirus
Mise à jour
Résident activé
Fichiers analysés 0
Fichiers infectés 0
Total messages reçus 0
Messages infectés 0
Dernière analyse du système jamais
Mise à jour automatique activée
Dernière mise à jour jamais
Signatures virales 145598
Version du moteur 7.01079
Bienvenue !
Des informations essentielles sur l'état de BitDefender sont affichées ici. Cochez ou décochez les cases à gauche afin d'activer ou désactiver les modules.
Les objets marqués en rouge demandent votre attention immédiate.
BitDefender est par défaut configuré pour une protection optimale.
Cliquez sur les onglets pour plus de détails ou pour modifier la configuration manuellement. Des informations détaillées sur chaque section seront toujours affichées ici.
Plus d'infos
bitdefender

Figure 9

En cochant ou décochant les cases, vous pouvez activer ou désactiver certaines des principales fonctions de BitDefender.

Les points marqués en rouge nécessitent votre attention immédiate.

Résident

Il fournit une protection permanente en temps réel contre les virus et autres menaces. Cette rubrique affiche le nombre de fichiers analysés, le nombre de fichiers infectés, le nombre d'emails analysés et d'emails infectés, ainsi que la date de la dernière analyse du système.

Pour prévenir l'infection de votre ordinateur par des virus, laissez le **Résident** activé.

Astuce: Nous vous recommandons fortement d'analyser complètement au moins une fois par semaine votre système. Pour cela, accédez au module **Antivirus**, section Analyse, cochez **Disques Locaux** puis cliquez sur **Analyse**.

Mise à jour automatique

De nouveaux virus sont identifiés chaque jour. C'est pourquoi il est très important de garder BitDefender à jour avec les dernières signatures de virus. Cette rubrique affiche la date de dernière mise à jour et le nombre de virus détectables par votre version de BitDefender.

Pour protéger vos données critiques, BitDefender peut réaliser des mises à jour automatiques. Laissez l'option **Mise à jour Automatique** activé.

Enregistrement du produit

Cette section contient des informations sur le statut de vos licences BitDefender. Vous pouvez ici enregistrer votre produit et voir sa date d'expiration.

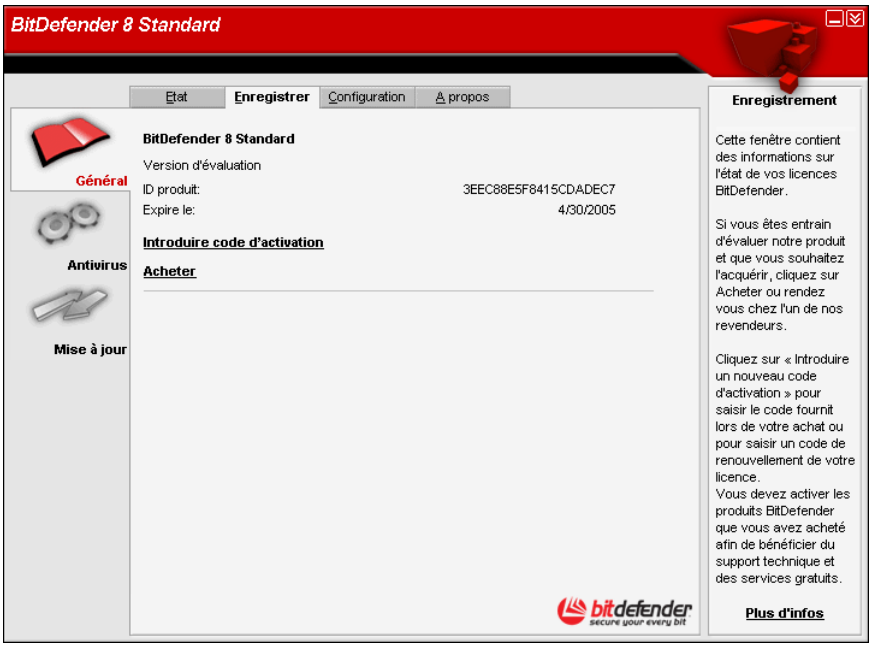

BitDefender 8 Standard
Etat
Enregistrer
Configuration
A propos
Général
Antivirus
Mise à jour
BitDefender 8 Standard
Version d'évaluation
ID produit:
3EEC88E5F8415CDADEC7
Expire le:
4/30/2005
Introduire code d'activation
Acheter
Enregistrement
Cette fenêtre contient des informations sur l'état de vos licences BitDefender.
Si vous êtes entrain d'évaluer notre produit et que vous souhaitez l'acquérir, cliquez sur Acheter ou rendez vous chez l'un de nos revendeurs.
Cliquez sur « Introduire un nouveau code d'activation » pour saisir le code fournit lors de votre achat ou pour saisir un code de renouvellement de votre licence.
Vous devez activer les produits BitDefender que vous avez acheté afin de bénéficier du support technique et des services gratuits.
Plus d'infos
bitdefender
secure your every bit

Figure 10

Cette section contient des informations sur le statut de vos licences BitDefender. Vous pouvez ici enregistrer votre produit et voir sa date d'expiration.

Le produit est livré par défaut avec un code d'évaluation valable 30 jours. A la fin de cette période d'essai, si vous souhaitez acheter le produit, vous pouvez cliquer sur le bouton **Acheter** ou vous rendre chez l'un de nos revendeurs.

Pour modifier la licence par défaut, cliquez sur **Introduir code d'activation**. La fenêtre suivante apparaîtra:

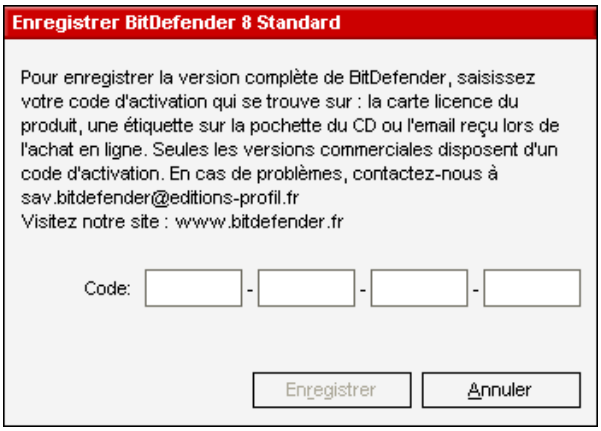

Enregistrer BitDefender 8 Standard
Pour enregistrer la version complète de BitDefender, saisissez votre code d'activation qui se trouve sur : la carte licence du produit, une étiquette sur la pochette du CD ou l'email reçu lors de l'achat en ligne. Seules les versions commerciales disposent d'un code d'activation. En cas de problèmes, contactez-nous à sav.bitdefender@editions-profil.fr
Visitez notre site : www.bitdefender.fr
Code:
Enregistrer
Annuler

Figure 11

Saisissez votre code dans le champ **Code** et cliquez sur **Enregistrer** pour finir l'enregistrement.

Si vous faîtes une erreur de saisie, il vous sera demandé de la re-rentrer.

Si vous entrez un code d'activation valide, une boîte de dialogue vous le confirmera.

Dans la section **Enregistrement**, vous pourrez voir à présent la date d'expiration de votre nouveau code d'activation.

Astuce: Merci d'activer le produit BitDefender que vous avez acheté pour pouvoir bénéficier du support technique et des services BitDefender.

Paramétrages de la console de contrôle

Vous pouvez dans cette rubrique paramétrer le fonctionnement de BitDefender. Par défaut, BitDefender est chargé au démarrage de Windows et se réduit automatiquement.

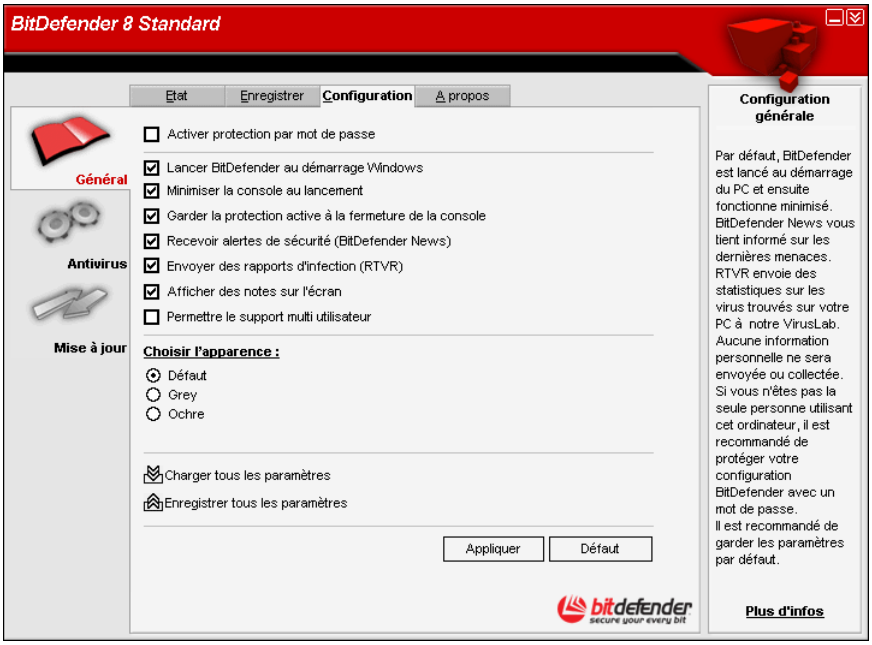

BitDefender 8 Standard
Etat
Enregistrer
Configuration
A propos
Général
Antivirus
Mise à jour
Activer protection par mot de passe
Lancer BitDefender au démarrage Windows
Minimiser la console au lancement
Garder la protection active à la fermeture de la console
Recevoir alertes de sécurité (BitDefender News)
Envoyer des rapports d'infection (RTVR)
Afficher des notes sur l'écran
Permettre le support multi utilisateur
Choisir l'apparence :
Défaut
Grey
Ochre
Charger tous les paramètres
Enregistrer tous les paramètres
Appliquer
Défaut
Configuration générale
Par défaut, BitDefender est lancé au démarrage du PC et ensuite fonctionne minimisé. BitDefender News vous tient informé sur les dernières menaces. RTVR envoie des statistiques sur les virus trouvés sur votre PC à notre VirusLab. Aucune information personnelle ne sera envoyée ou collectée. Si vous n'êtes pas la seule personne utilisant cet ordinateur, il est recommandé de protéger votre configuration BitDefender avec un mot de passe. Il est recommandé de garder les paramètres par défaut.
Plus d'infos

Figure 12

Pour choisir une option, cliquez simplement sur la case correspondante.

➔ **Activer protection par mot de passe** – permet de choisir un mot de passe afin de protéger la configuration choisie pour BitDefender.

Si vous n'êtes pas le seul utilisateur de votre ordinateur, il est recommandé de protéger vos paramétrages BitDefender par un mot de passe.

La fenêtre suivante apparaîtra:

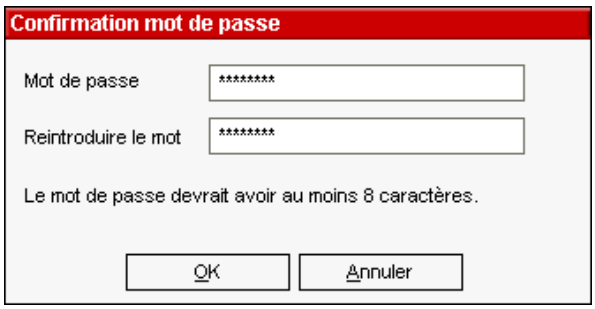


Figure 13

Entrez le mot de passe dans le champ **Mot de passe**, re-saisissez le dans le champ **Reintroduire le mot** de passe et cliquez sur **OK**.

A présent, si vous souhaitez changer les options de configuration de BitDefender, le mot de passe vous sera demandé.

Si vous oubliez le mot de passe, vous devrez réparer le produit afin de pouvoir modifier la configuration de BitDefender.

- **Lancer BitDefender au démarrage Windows** – lance automatiquement BitDefender au démarrage du système. Cela est fortement recommandé!
- **Minimiser la console au lancement** – réduit la console de management BitDefender après son chargement au démarrage. Seul l'icône BitDefender apparaîtra dans la zone de notification.
- **Garder la protection à la fermeture de la console** – même si la console est fermée (plus apparente dans la zone de notification), BitDefender continuera à vous protéger.
- **Recevoir alertes de sécurité** – affiche régulièrement des informations de sécurité sur des risques de virus et/ou de failles, envoyées par serveurs de BitDefender.
- **Afficher l'écran d'accueil**– montre l'écran qui apparaît lorsque vous lancez BitDefender.
- **Envoyer des rapports d'infection**– envoie au laboratoire BitDefender des rapports concernant les virus identifiés sur vote PC.

  Le rapport ne contiendra aucune donnée confidentielle, comme votre nom, votre adresse IP ou autre et ne sera pas utilisé à des fins commerciales. Les informations envoyées contiendront seulement le nom des virus et seront utilisées pour créer des rapports statistiques.
- **Afficher des notes sur l'écran** – affiche des fenêtres d'alertes sur les statuts de votre produit.
- **Permettre le support multi utilisateur** – permet aux autres utilisateurs du même ordinateur de garder leur configuration pour BitDefender.

Note

Cet option peut être activée ou pas par les utilisateurs ayant des droits d'administrateur sur la machine locale.

- L'option **Choisir l'apparence** vous permet de sélectionner la couleur de la console de management. Le skin représente l'image de fond de l'interface. Pour sélectionner un skin différent, cliquez sur la couleur correspondante.

Utilisez les boutons **Sauvegarder Tous les paramètres** / **Charger Tous les Paramètres** pour sauvegarder ou charger les paramètres établis pour BitDefender dans un endroit spécifié. Ainsi, vous pouvez utiliser les mêmes paramètres après la réinstallation ou la réparation de votre BitDefender.

Cliquez sur **Appliquer** pour enregistrer les modifications. Si vous cliquez sur **Défaut** vous allez charger les paramètres par défaut.

A propos

Dans cette section vous pouvez trouver des informations sur votre produit et les contacts dont vous pourriez avoir besoin.

BitDefender™ fournit des solutions de sécurité pour satisfaire les besoins de protection des environnements informatiques actuels et protège actuellement plus de 120 millions d'utilisateurs particuliers ou professionnels dans plus de 100 pays.

BitDefender™ est certifié par tous les principaux organismes de tests indépendants - **ICSA Labs**, **CheckMark**, **Virus Bulletin** et **TUV**, et est la seule solution de sécurité à avoir reçu le prix européen de l'innovation technologique **IST Prize**.

Module Antivirus

BitDefender vous protège contre les codes malveillants tentant d'entrer dans votre système en scannant vos fichiers, emails, téléchargements et tout autre contenu dès qu'il entre sur votre PC.

Plus de fonctions

Depuis le module Antivirus vous accédez à l'ensemble des paramétrages et fonctions antivirus de BitDefender.

Analyse à l'accès et **Analyse à la demande**

La protection antivirus est divisée en deux catégories:

- Analyse à l'accès: Empêche l'intrusion de nouveaux virus dans votre système. Cela est également appelé un résident. Les fichiers sont scannés dès que l'utilisateur tente d'y accéder. BitDefender analysera, par exemple, un document « Word » lorsque vous l'ouvrirez, et un email lorsque vous en recevrez un. BitDefender analyse ainsi les fichiers « comme vous les utilisez » - à l'accès.

- Analyse à la demande: Détecte des virus déjà présent sur votre système. C'est la classique analyse antivirus déclenchée par l'utilisateur – vous choisissez quel disque, répertoire ou fichier que BitDefender devrait analyser, et BitDefender le scanne – à la demande.

Des explications complémentaires de ces types d'analyses sont présentées dans les chapitres suivants.

Analyse à l'accès

Dans le cas où vous n'auriez pas encore ouvert la console de management, vous pouvez y accéder depuis le menu Démarrer de Windows en suivant le chemin suivant **Démarrer → Programmes → BitDefender → BitDefender 8 Standard** ou plus rapidement en double-cliquant sur l'icône BitDefender dans la zone de notification.

Dans la console, cliquez sur **Antivirus**.

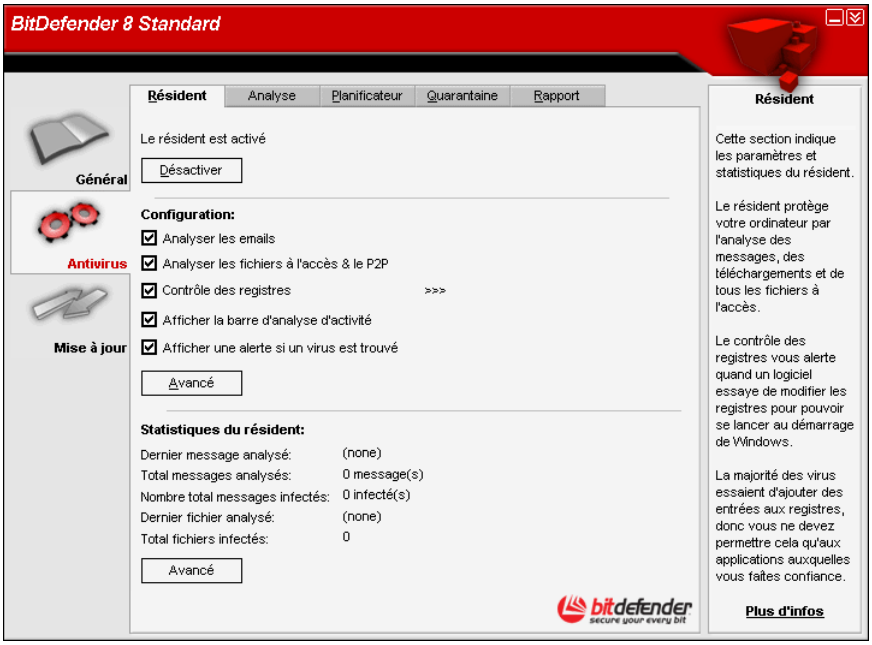

BitDefender 8 Standard
Résident
Analyse
Planificateur
Quarantaine
Rapport
Général
Antivirus
Mise à jour
Le résident est activé
Désactiver
Configuration:
Analyser les emails
Analyser les fichiers à l'accès & le P2P
Contrôle des registres
>>>
Afficher la barre d'analyse d'activité
Afficher une alerte si un virus est trouvé
Avancé
Statistiques du résident:
Dernier message analysé: (none)
Total messages analysés: 0 message(s)
Nombre total messages infectés: 0 infecté(s)
Dernier fichier analysé: (none)
Total fichiers infectés: 0
Avancé
bitdefender
secure your every bit
Résident
Cette section indique les paramètres et statistiques du résident.
Le résident protège votre ordinateur par l'analyse des messages, des téléchargements et de tous les fichiers à l'accès.
Le contrôle des registres vous alerte quand un logiciel essaye de modifier les registres pour pouvoir se lancer au démarrage de Windows.
La majorité des virus essaient d'ajouter des entrées aux registres, donc vous ne devez permettre cela qu'aux applications auxquelles vous faites confiance.
Plus d'infos

Figure 14

Le **Résident** protège votre ordinateur en analysant les emails, téléchargements et tous les fichiers à l'accès.

Pour prévenir l'infection de votre ordinateur par des virus, garder le **Résident** activé.

En bas de cette section, vous pouvez voir les statistiques de BitDefender sur les fichiers et emails. Cliquez sur **Avancé** si vous voulez une fenêtre plus détaillée au sujet de ces statistiques.

Avec les paramétrages, vous pouvez personnaliser ce que BitDefender doit analyser à l'accès et comment il doit réagir s'il rencontre un virus.

Contrôle des registres

Une partie très importante du système d'exploitation Windows est appelée la **Base de registres**. C'est l'endroit où Windows conserve ses paramétrages, programmes installés, informations sur l'utilisateur et autres.

La **Base de registres** est également utilisée pour définir quels programmes devraient être lancés automatiquement lorsque Windows démarre. Cela est souvent utilisé par les virus afin d'être automatiquement lancé lorsque l'utilisateur redémarre son ordinateur.

Le **Contrôle des registres** garde un oeil sur les registres Windows – c'est également utile pour détecter des chevaux de Troie. Il vous alertera dès qu'un programme essaiera de modifier une entrée dans la base de registres afin de s'exécuter au démarrage de Windows.

Figure 15

Vous pouvez refuser cette modification en cliquant sur **Non** ou l'autoriser en cliquant sur **Oui**. Si vous souhaitez que BitDefender se souvienne de votre réponse, cochez la case: **Retenir cette réponse**.

Vos réponses seront la base de la liste de règles.

Si vous souhaitez voir la liste des entrées dans la base de registres, cliquez sur >>> dans **Contrôle des registres**.

La fenêtre suivante apparaîtra:

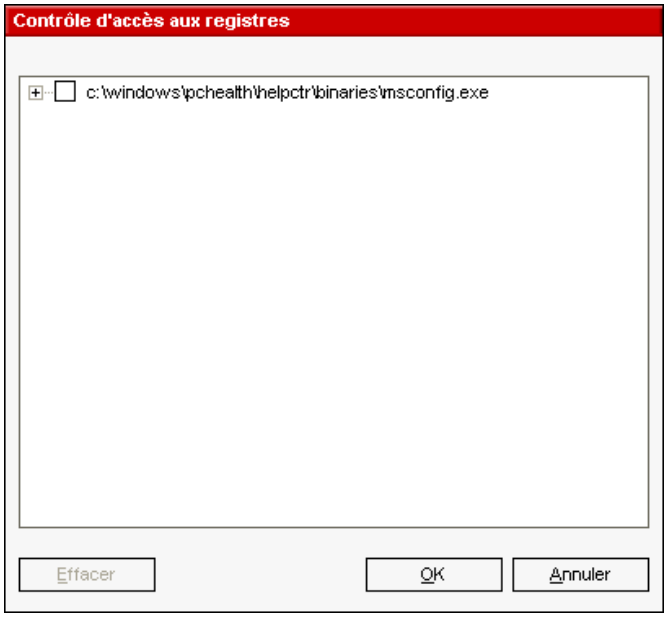


Figure 16

Pour chaque application, un menu extensible sera créé; il contient toutes les modifications des registres.

Pour supprimer une entrée dans les registres, sélectionnez la et cliquez sur **Supprimer**.

Pour désactiver temporairement une entrée sans la supprimer, décochez la case qui est devant ☑ en cliquant dessus. Lorsque l'entrée est désactivée, la case ressemblera à cela ☐.

Note

BitDefender vous alertera à l'installation de nouveaux logiciels nécessitant d'être lancé après le prochain démarrage de votre ordinateur. Dans la plupart des cas, ces programmes sont légitimes et peuvent être autorisés.

Sélectionner les principaux paramétrages

Pour choisir une option, cliquez avec la souris sur la case correspondante:

- **Analyser les emails** – tous les emails seront analysés par BitDefender. Cela est hautement recommandé!
- **Analyser les fichiers à l'accès & le P2P**– tous les fichiers à l'accès sont analysés par BitDefender.
- **Afficher la barre d'analyse d'activité** – décochez cette option si vous ne souhaitez plus voir la barre d'analyse d'activité.
- **Afficher une alerte si un virus est trouvé** –une fenêtre d'alerte sera affichée lors de la rencontre d'un virus dans un fichier ou message e-mail.

  Pour un fichier infecté, la fenêtre d'alerte va contenir le nom du virus, le chemin, l'action effectuée par BitDefender et un lien vers le site BitDefender où on peut trouver plus d'informations sur celui-ci. Pour un message e-mail infecté, la fenêtre d'alerte va contenir aussi l'information sur l'expéditeur et le destinataire.

  Au cas où un fichier suspect est détecté vous pouvez lancer un assistant à partir de la fenêtre d'alerte qui vous aidera envoyer ce fichier au Laboratoire BitDefender pour une analyse ultérieure. Vous pouvez saisir votre adresse email pour recevoir des informations sur ce rapport.

Sélectionner d'autres options

Cliquez sur **Avancé** pour sélectionner les objets que vous souhaitez analyser et l'action à entreprendre sur les fichiers infectés. La fenêtre apparaîtra:

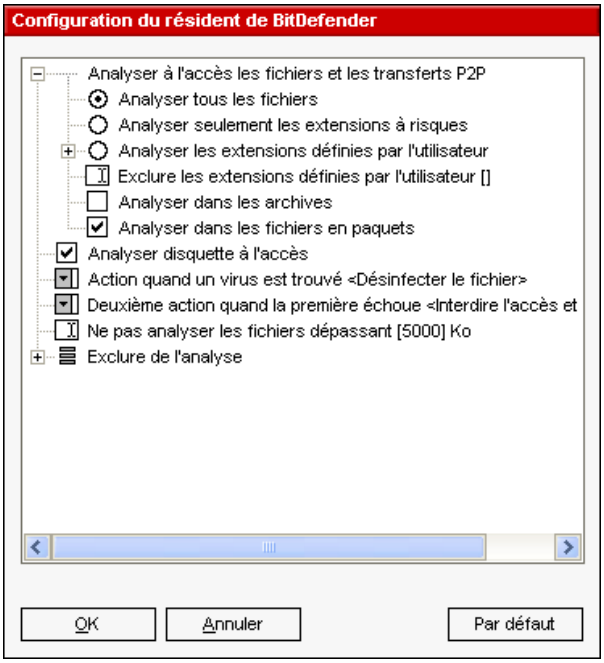

Configuration du résident de BitDefender
Analyser à l'accès les fichiers et les transferts P2P
Analyser tous les fichiers
Analyser seulement les extensions à risques
Analyser les extensions définies par l'utilisateur
Exclure les extensions définies par l'utilisateur []
Analyser dans les archives
Analyser dans les fichiers en paquets
Analyser disquette à l'accès
Action quand un virus est trouvé <Désinfecter le fichier>
Deuxième action quand la première échoue <Interdire l'accès et
Ne pas analyser les fichiers dépassant [5000] Ko
Exclure de l'analyse
OK
Annuler
Par défaut

Figure 17

Cliquez la case avec "+" pour ouvrir une option ou la case avec "-" pour fermer une option.

Vous pouvez observer que certaines options d'analyse, bien que le signe "+" apparaisse, ne peuvent s'ouvrir. La raison est que ces options n'ont pas encore été sélectionnées. Vous observerez que si vous les cochez, elles pourront être ouvertes.

- Sélectionner **Analyser à l'accès les fichiers et les transferts P2P** pour analyser les fichiers à l'accès ainsi que les communications et échanges Peer To Peer (messageries instantanées comme ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger – logiciels de téléchargement comme Kazaa, Emule, Shareaza). Après cela, sélectionnez le type de fichiers que vous voulez analyser.

Les options suivantes sont disponibles:

Option	Description
Analyse de tous les fichiers	Tous les fichiers à l'accès seront analysés, quelque soit leur type.
Analyse seulement les extensions à risques	Seuls les fichiers avec les extensions suivantes seront analysés: `exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pfd; msi; ini; csc; cmd; bas; eml; nws.`
Analyse les extensions définies par l'utilisateur	Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par ";".
Exclure les extensions définies par l'utilisateur	Tous les fichiers à l'accès seront analysés à l'exception de ceux avec des extensions définies par l'utilisateur. Ces extensions doivent être séparées par ";".
Analyser dans les archives	Les archives serons également analysées.
Analyser dans les fichiers en paquets	Tous les fichiers en paquets seront analysés.

➔ Sélectionnez **Analyse disquette à l'accès** si vous souhaitez analyser les disquettes à l'accès.

➔ Cliquez sur la rubrique **Action quand un virus est trouvé** et sélectionnez dans la liste la première action sur les fichiers infectés.

BitDefender permet de sélectionner deux actions dans le cas où un fichier infecté est trouvé. La seconde action n'est activée que dans le cas où la première action sélectionnée est de désinfecter les fichiers infectés. Vous pouvez sélectionner l'une des actions suivantes:

Première action	Description
Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.
Désinfecter le fichier	Pour désinfecter un fichier infecté.
Effacer le fichier	Supprimer un fichier infecté, sans alerte.
Déplacer en quarantine	Les fichiers infectés sont déplacés en quarantaine. Lorsque le virus est en quarantaine il ne peut avoir aucune action néfaste.

➔ Cliquez sur la rubrique **Deuxième action quand la première échoue** et sélectionnez dans la liste la seconde action sur les fichiers infectés.

Les options suivantes sont disponibles.

Deuxième action	Description
Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.
Effacer le fichier	Supprimer un fichier infecté, sans alerte.
Déplacer en quarantine	Les fichiers infectés sont déplacés en quarantaine. Lorsque le virus est en quarantaine il ne peut avoir aucune action néfaste.

➔ Cliquez sur **Ne pas analyser les fichiers dépassant** à et tapez la taille maximum des fichiers à analyser. Si vous mettez la taille à 0, tous les fichiers seront analysés.

➔ Cliquez sur "+" dans **Exclure de l'analyse** afin de spécifier un répertoire qui sera exclu de l'analyse. La conséquence sera d'ajouter une nouvelle option, **Nouveau choix**. Cliquez sur la boîte correspondante à ce nouveau choix et à partir de la fenêtre d'exploration, sélectionnez le répertoire que vous souhaitez exclure de l'analyse.

Cliquez sur **OK** pour enregistrer les modifications. Si vous cliquez sur **Par Défaut** vous allez charger les paramètres par défaut.

Analyse à la demande

L'objectif principal de BitDefender est de conserver votre PC sans virus. Cela est assuré avant tout par l'analyse antivirus des emails que vous recevez et des fichiers que vous téléchargez ou copiez sur votre système.

Il y a cependant un risque qu'un virus soit déjà logé dans votre système, avant même l'installation de BitDefender. C'est pourquoi il est prudent d'analyser votre ordinateur après l'installation de BitDefender et c'est encore plus prudent d'analyser régulièrement votre ordinateur contre les virus.

BitDefender permet quatre types d'analyse à la demande:

- Analyse immédiate – il y a quelques étapes à suivre pour analyser votre ordinateur contre les virus;
- Analyse contextuelle – un clic-droit sur un fichier ou répertoire permet de sélectionner **BitDefender Antivirus v8**;
- Analyse par glisser & déposer – glissez & déposez un fichier ou un répertoire sur la barre d'analyse d'activité;
- Analyse programée – vous pouvez programmer BitDefender pour analyser votre système contre les virus périodiquement.

Analyse immédiate

Pour analyser votre ordinateur contre les virus, veuillez suivre les étapes suivantes:

1. Fermez tous les programmes ouverts

Afin de permettre à BitDefender de réaliser une analyse complète, il est nécessaire de fermer tous les programmes ouverts, tout spécialement les clients de messagerie (ex : Outlook, Outlook Express ou Eudora).

2. Vérifiez que BitDefender est à jour contre les derniers virus

Avant de laisser BitDefender analyser votre ordinateur, vous devriez vérifier que BitDefender est à jour de ses signatures de virus, dans la mesure où de nouveaux virus apparaissent chaque jour. Vous pouvez vérifier de quand date la dernière mise à jour en bas du module Mise à jour de la **console de management BitDefender**.

Si cette date n'est pas récente, vous devriez laisser BitDefender mettre à jour ses signatures de virus. C'est très simple, tout ce que vous avez à faire et de cliquez sur le bouton **Vérification** dans le module Mise à jour.

3. Choisissez la cible de l'analyse

Dans la console de management, entrez dans le module Antivirus et cliquez sur l'onglet Analyse. Par défaut, la section contient une image de la structure des partitions du système. A côté de cela, des boutons et options d'analyse peuvent également être observés.

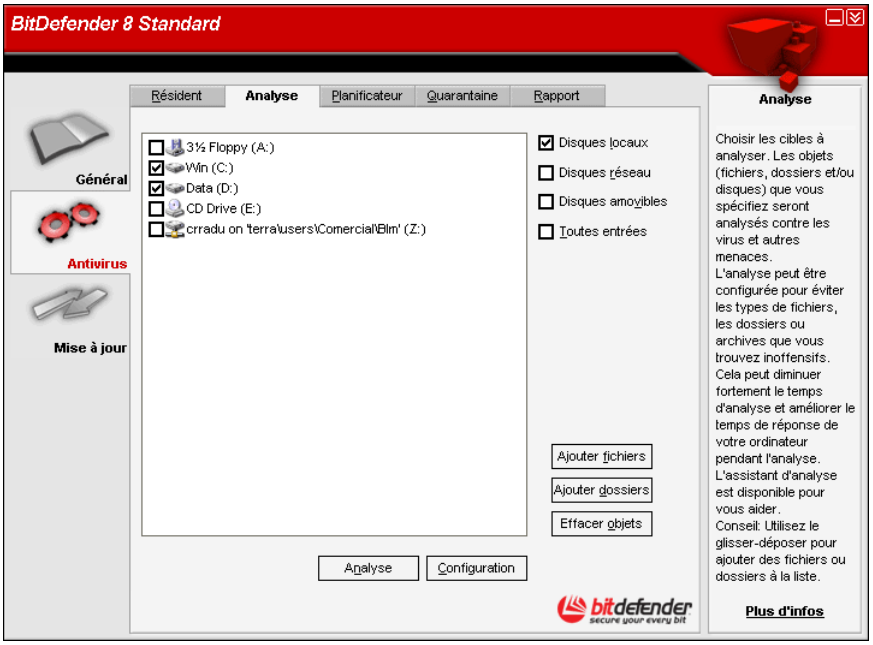

BitDefender 8 Standard
Résident
Analyse
Planificateur
Quarantaine
Rapport
Général
Antivirus
Mise à jour
3½ Floppy (A:)
Win (C:)
Data (D:)
CD Drive (E:)
crradu on 'terra\users\Comercial\Blm' (Z:)
Disques locaux
Disques réseau
Disques amovibles
Toutes entrées
Ajouter fichiers
Ajouter dossiers
Effacer objets
Analyse
Configuration
Analyse
Choisir les cibles à analyser. Les objets (fichiers, dossiers et/ou disques) que vous spécifiez seront analysés contre les virus et autres menaces.
L'analyse peut être configurée pour éviter les types de fichiers, les dossiers ou archives que vous trouvez inoffensifs. Cela peut diminuer fortement le temps d'analyse et améliorer le temps de réponse de votre ordinateur pendant l'analyse.
L'assistant d'analyse est disponible pour vous aider.
Conseil: Utilisez le glisser-déposer pour ajouter des fichiers ou dossiers à la liste.
Plus d'infos

Figure 18

La section contient les boutons suivants:

- **Ajouter fichiers** - le bouton qui permet de rajouter des fichiers pour l'analyse. En cliquant dessus, une fenêtre de navigation s'ouvre et vous pouvez choisir le fichier.
- **Ajouter dossiers** - le bouton qui permet de rajouter un nouveau dossier pour l'analyse. En cliquant dessus, une fenêtre de navigation s'ouvre et vous pouvez choisir le dossier.

  Astuce: Vous pouvez rajouter des fichiers et des dossiers à la liste d'analyse en les glissant-déposant sur la section **Analyse**.

- **Effacer sélection** - efface le fichier/dossier sélectionné auparavant.

  Seulement les fichiers/dossiers rajoutés après peuvent être effacés, mais pas ceux qui sont automatiquement "proposés" par BitDefender.

➔ **Paramétrages** – ouvre une fenêtre dans laquelle vous pouvez spécifier quels types de fichiers sont à analyser, l'action sur les fichiers infectés, la génération de messages d'alertes, la sauvegarde des résultats d'analyse dans des fichiers rapports.
➔ **Analyse** - lance l'analyse en tenant compte des options choisies.

Ces options permettent une sélection rapide des cibles d'analyses:

- **Disques locaux** – pour analyser les disques locaux.
- **Disques réseaux** – pour analyser tous les lecteurs réseaux.
- **Disques amovibles** – pour analyser les disques amovibles (CD-ROM, lecteur de disquettes).
- **Toutes les entrées** – pour analyser l'ensemble des lecteurs, peu importe qu'ils soient locaux, réseaux ou amovibles.

Si vous voulez analyser l'ensemble de votre ordinateur, cochez la case **Toutes les entrées**.

Si vous n'êtes pas habitué à paramétrer, vous pouvez à présent cliquer sur le bouton **Analyse**. BitDefender commencera l'analyse de votre PC avec les paramétrages standard, qui sont suffisants.

4. Sélectionnez les options d'analyse – seulement pour les utilisateurs avancés

Les utilisateurs avancés peuvent vouloir tirer avantage des possibilités de paramétrage d'analyse de BitDefender. Le scanner peut être paramétré pour éviter certaines extensions de fichiers, répertoires ou archives que vous savez être sans danger. Cela peut considérablement réduire le temps d'analyse et améliorer le temps de réaction de votre ordinateur durant une analyse.

Explorez cela en cliquant sur l'onglet **Configuration**.

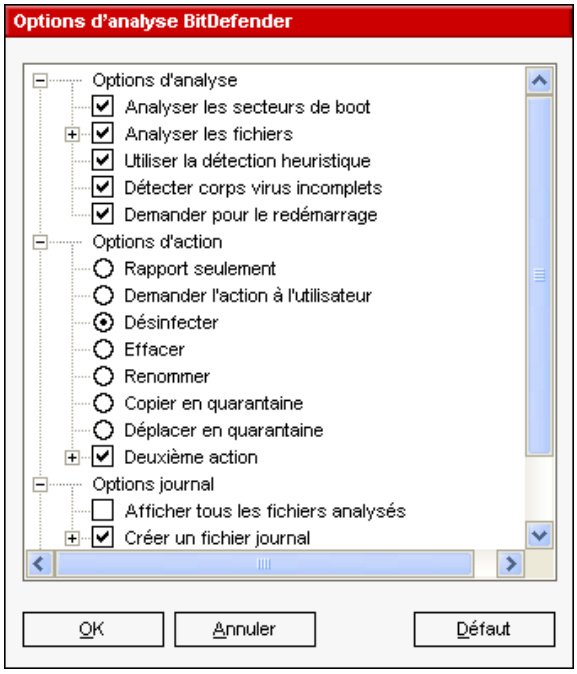


Figure 19

Les options d'analyse sont organisés en menus extensibles très proche de ceux qui sont utilisés dans l'explorateur Windows.

Les options d'analyse sont groupées en quatre catégories:

- **Options d'analyse**
- **Options d'action**
- **Options jurnal**
- **Options de performance**

Cliquez sur la case avec un "+" pour ouvrir une option et sur la case avec un "-" pour fermer une option.

L'étape suivante permet de spécifier le type d'objets à analyser (archives, e-mail et autres) et permet d'activer l'analyse heuristique (pour détecter des virus encore inconnus). Cela est réalisé par la sélection de certaines options dans la catégorie **Options d'analyse**.

Les options suivantes sont disponibles:

Option		Description
Analyser les secteurs de boot		Pour analyser les secteurs de boot du système.
Analyser les fichiers	Analyser tous les fichiers	Pour analyser tous les fichiers, quelque soit leur type.
	Analyser seulement les extensions à risques	Pour analyser seulement les fichiers avec les extensions suivantes: `exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pfd; msi; ini; csc; cmd; bas; eml; nws.`
	Analyser les extensions définies par l'utilisateur	Pour analyser seulement les fichiers avec les extensions définies par l'utilisateur. Ces extensions doivent être séparées par ";".
	Exclure les extensions définies par l'utilisateur	Pour analyser tous les fichiers, à l'exception de ceux avec des extensions définies par l'utilisateur. Ces extensions doivent être séparées par ";".
	Ouvrir les paquets programmes	Analyser les fichiers en paquets.
	Ouvrir les archives	Analyser l'intérieur des archives.
	Ouvrir les archives des messagerie	Analyser dans les archives de messagerie.
Utiliser la détection heuristique		Active l'analyse heuristique des fichiers. Le but de l'analyse heuristique est d'identifier de nouveaux virus, se basant sur des algorithmes spécifiques, avant que ces virus soient connus. De fausses alertes peuvent apparaître et cette méthode ne peut pas garantir un taux de détection à 100% de ces nouveaux virus. Quand un tel fichier est détecté il est classifié comme étant suspect. Dans ce cas, nous vous recommandons d'envoyer le fichier au laboratoire BitDefender afin qu'il soit analysé.

Ensuite vous devez spécifier **l'action à appliquer aux fichiers suspects et infectés**. L'action peut être sélectionnée dans la catégorie **Options d'action**. Cliquez sur le "+" pour l'ouvrir et voir toutes les actions possibles sur les fichiers infectés.

Vous pouvez sélectionner l'une des suivantes:

Action	Description
Rapport seulement	Pour rapporter la détection d'un fichier infecté et le nom du virus.
Demander l'action à l'utilisateur	Quand un fichier infecté est détecté, une fenêtre apparaît, demandant à l'utilisateur de choisir une action à appliquer au fichier. Suivant l'importance du fichier, vous pouvez choisir de le désinfecter, l'isoler en quarantaine ou l'effacer.
Désinfecter	Pour désinfecter les fichiers infectés.
Effacer	Pour effacer les fichiers infectés.
Renommer	Pour renommer les fichiers infectés.
Copier en quarantaine	Pour copier les fichiers infectés dans la zone de quarantaine. Cela revient concrètement à dupliquer le fichier infecté dans la zone de quarantaine, mais le fichier infecté ne sera pas retiré de son emplacement d'origine.
Déplacer en quarantaine	Déplacer les fichiers infectés dans la zone de quarantaine. Lorsque le virus est en quarantaine il ne peut faire aucun dégat.
Deuxième action	Cliquez sur cette option si vous désirez sélectionner la deuxième action à appliquer aux fichiers infectés. Ceci n'est possible que si la première action choisie est "Désinfecter".

Pour sélectionner la deuxième action à appliquer, cliquez sur le "+", après avoir coché **Deuxième action**.

Les options disponibles en deuxième action sont décrites dans le tableau ci-dessous.

Action	Description
Rapport seulement	Pour rapporter la détection d'un fichier infecté et le nom du virus.
Demander l'action à l'utilisateur	Quand un fichier infecté est détecté, une fenêtre apparaît, demandant à l'utilisateur de choisir une action à appliquer au fichier. Suivant l'importance du fichier, vous pouvez choisir de le désinfecter, l'isoler en quarantaine ou l'effacer.
Effacer	Pour effacer les fichiers infectés.
Renommer	Pour renommer les fichiers infectés.
Copier en quarantaine	Pour copier les fichiers infectés dans la zone de quarantaine. Cela revient concrètement à dupliquer le fichier infecté dans la zone de quarantaine, mais le fichier infecté ne sera pas retiré de son emplacement d'origine.
Déplacer en quarantaine	Déplacer les fichiers infectés dans la zone de quarantaine. Lorsque le virus est en quarantaine il ne peut faire aucun dégat.

L'étape suivante est la sélection des options journal. Vous devez cliquer sur le signe "+" correspondant aux **Options journal**. Ces options permettent l'activation des alertes et la création des fichiers journal (contenant des informations sur l'analyse).

Option		Description
Afficher tous les fichiers analysés		Affiche tous les fichiers, infectés ou pas, et leur état dans un fichier journal.
Créer un fichier journal	Nom du fichier rapport	Ceci est un champ qui permet le changement du nom du fichier rapport. Vous devez simplement cliquer sur cette option et introduire un nouveau nom.
	Ajouter au rapport existant	Choisissez cette option pour ajouter les informations sur la dernière analyse à la fin du journal, après celles déjà existantes.
	Limiter la taille du journal à [x] Ko	Cliquez sur cette option et introduisez la taille maximum du fichier dans le champ qui apparaît.

Dans la catégorie **Options de performance** vous pouvez décroître la priorité du processus d'analyse. Si vous cochez la case **Exécuter la tâche d'analyse avec une priorité basse** vous allez permettre aux autres logiciels d'être exécutés à une vitesse supérieure et d'augmenter le temps nécessaire pour le final du processus d'analyse.

Astuce: Vous pouvez voir le fichier de rapport dans la section Rapport du module **Antivirus**.

Note

Vous pouvez observer que certaines options d'analyse, bien que le signe "+" apparaisse, ne peuvent s'ouvrir. La raison est que ces options n'ont pas encore été sélectionnées. Vous observerez que si vous les cochez, elles pourront être ouvertes.

Cliquez sur **OK** pour enregistrer les modifications. Si vous cliquez sur **Défaut** vous allez charger les paramètres par défaut.

5. Analyse virale

Une fois les options d'analyse choisies, tout ce qu'il vous reste à faire est de démarrer l'analyse. Pour le faire, cliquez sur **Analyse**. Cela peut durer un certain temps, suivant la taille de votre disque.

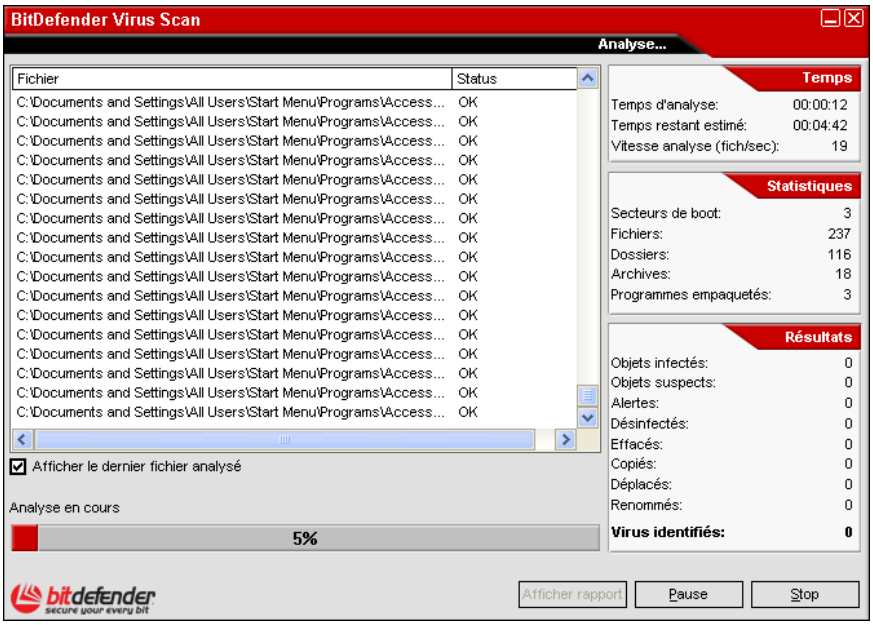


Figure 20

Durant l'analyse, BitDefender vous montrera sa progression et vous alertera si le moindre virus est trouvé.

Cochez la case correspondante à **Afficher le dernier fichier analysé** et seulement les informations sur les derniers fichiers analysés seront visibles.

Si vous cliquez:

- **Stop** - une nouvelle fenêtre s'affichera vous permettant de stopper la vérification du système. Si vous choisissez d'arrêter, le bouton **Stop** se transformera en un bouton **Fermer** et le chosir fermera la fenêtre d'analyse.
- **Pause** - l'analyse s'arrête temporairement – vous pouvez la continuer en cliquant sur **Poursuivre**.
- **Afficher le rapport** – le rapport d'analyse s'ouvre.

Le fichier rapport est sauvegardé automatiquement dans la section Rapport du module **Antivirus**.

Astuce: Afin de voir les fichiers analysés vous devez sélectionner l'option **Afficher tous les fichiers scannés** dans les options de rapport (étape précédente). Avec cette option activée, l'ordinateur sera ralentit.

6. Méthodes alternatives d'analyse

BitDefender propose deux méthodes alternatives pour l'analyse immédiate de fichiers : en utilisant le menu contextuel et par la fonction glisser & déposer.

Analyse contextuelle

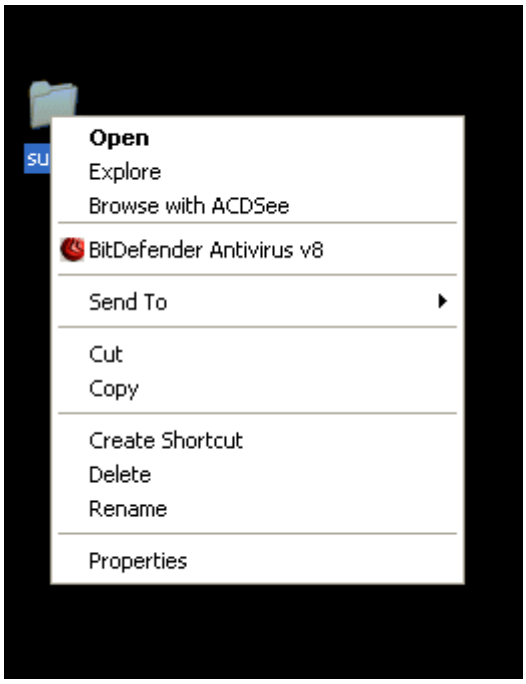


Figure 21

Faîtes un clic-droit sur le fichier ou répertoire que vous souhaitez analyser et sélectionnez l'option **BitDefender Antivirus v8**.

Un fichier rapport nommé `vscan.log` sera créé et accessible dans le module **Antivirus**, section Rapport.

Analyse par glisser & déposer

Glissez le fichier ou répertoire que vous voulez analyser et déposez le sur la **Barre d'analyse d'Activité**, comme sur l'image ci-dessous.

Figure 22

Figure 23

Un fichier rapport nommé `activbar.log` sera créé et accessible dans le module **Antivirus**, section Rapport.

Dans les deux cas, la fenêtre d'analyse (Figure 20) apparaîtra.
Si un virus est détecté, une fenêtre d'alerte (Figure 24) apparaîtra:

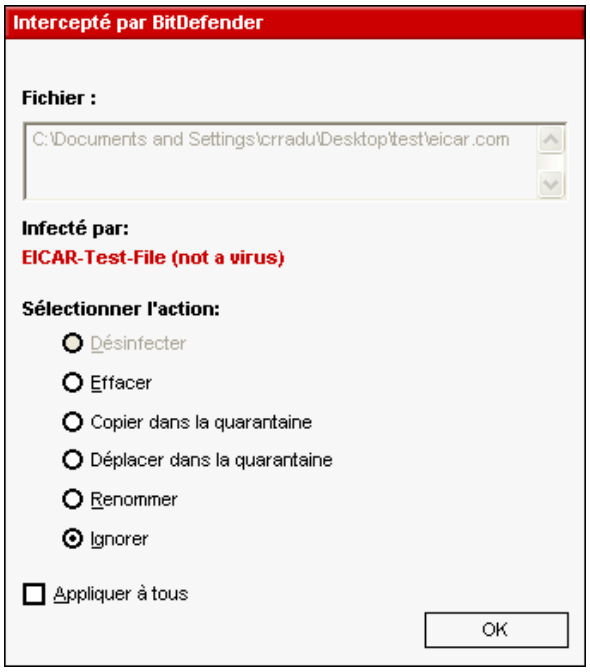


Figure 24

Vous pouvez voir le nom du fichier et le nom du virus.

Vous pouvez sélectionner une des options suivantes:

- **Désinfecter** - désinfecter le fichier infecté.
- **Effacer** - effacer le fichier infecté.
- **Copier en** quarantaine – copier le fichier infecté dans la zone de quarantaine.
- **Déplacer en** quarantaine – déplacer le fichier infecté dans la zone de quarantaine.
- **Renommer** - pour renommer le fichier infecté.
- **Ignorer** - ignorer l'infection. Aucune action ne sera appliquée au fichier infecté.

Si vous analysez un répertoire, et que vous souhaitez que l'action sur les fichiers infectés soit la même pour tous, cochez l'option **Appliquer à tous**.

Si l'option **Désinfecter** n'est pas activée, cela veut dire que le fichier ne peut pas être désinfecter. Le meilleur choix est alors de l'isoler en quarantaine et de nous l'envoyer, ou de le supprimer.

A la fin, cliquez sur **OK**.

Analyse programmée

Etant donné que l'analyse prendra du temps, et qu'elle fonctionnera mieux si vous avez fermé les autres programmes, il est préférable pour vous de programmer une analyse à une heure où vous n'utilisez pas votre ordinateur. Cela implique que l'utilisateur doit à l'avance créer une tâche.

Les fonctions suivantes sont disponibles:

- Assistant de création de tâches d'analyses programmées;
- Sélection de la fréquence d'analyse;
- Sélection des lecteurs et/ou répertoires;
- Sélection des extensions de fichiers;
- Possibilité de configuration distincte pour chaque tâche d'analyse;
- Possibilité d'analyse réseau (LAN);
- Isolation automatique en zone de quarantaine des fichiers infectés ou suspects;
- Analyse en tâche de fond sans interférence avec l'activité de l'utilisateur;
- Sommaire des propriétés des tâches programmées;
- Création de rapports d'analyse.

Dans la console de management, entrez dans le module **Antivirus** et cliquez sur l'onglet **Planificateur**.

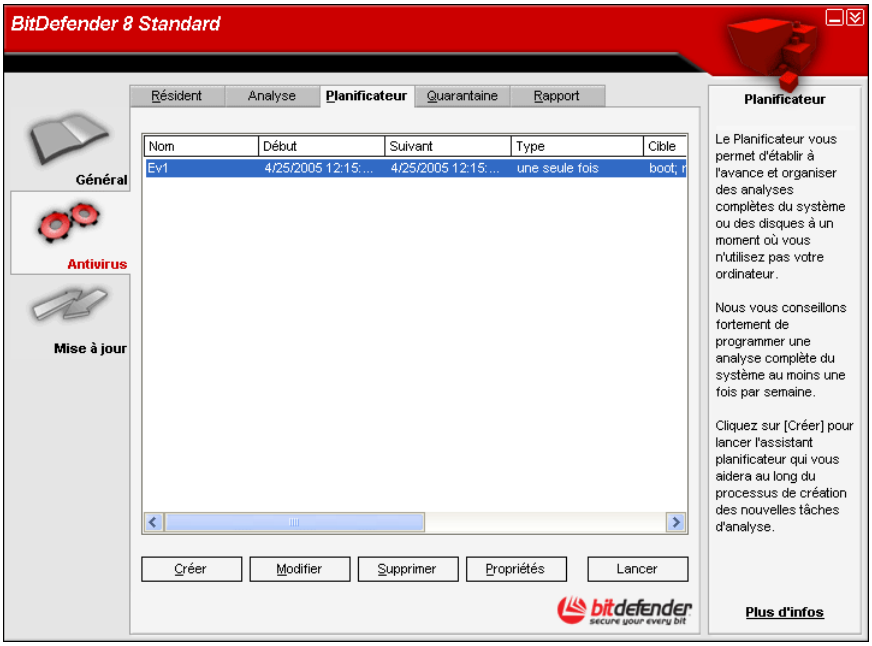


Figure 25

La section du **Planificateur** contient quelques boutons pour administrer les tâches d'analyse:

- Créér – lance l'assistant qui vous guidera dans la création d'une nouvelle tâche d'analyse.
- **Modifier** – modifie les propriétés d'une tâche précédemment créée. Cela lance également l'assistant.

> Si vous modifiez le nom d'un évènement, un nouvel évènement sera créé, sous le nouveau nom saisi.

- **Supprimer** – efface une tâche sélectionnée.
- **Propriétés** – affiche les propriétés d'une tâche sélectionnée.
- **Lancer** – démarre immédiatement la tâche choisie.

L'écran du **Planificateur** contient également une liste où toutes les tâches peuvent être vues, avec leur nom, la date de première exécution, la date de la prochaine exécution et son type (périodique ou une fois seulement).

Le **Planificateur** intègre un assistant de création de nouvelles tâches d'analyse. Il vous assistera chaque fois que vous aurez besoin de faire une opération sur ces évènements, que ce soit pour créer une nouvelle tâche ou pour en modifier une existante.

Cliquez sur Créér. Cela lancera l'assistant de création de tâches.

Astuce: Nous vous recommandons fortement de programmer une analyse complète du système au moins une fois par semaine.

1. Spécifier le nom de la tâche

Il vous faut tout d'abord spécifier un nom pour la nouvelle tâche.

Tapez le nom du nouvel évènement dans le champ **Nom tâche** et un court descriptif dans le champ **Description tâche**.

Cochez la case **Lévénement aura une basse priorité** si vous désirez diminuer la priorité de la tâche d'analyse et permettre aux autres logiciels d'être exécutés plus rapidement. Cela augmentera le temps nécessaire pour la fin de la tâche.

Figure 26

Cliquez sur **Suivant** pour continuer. Si vous cliquez sur **Annuler** une fenêtre apparaîtra pour vous demander confirmation.

2. Sélectionner la fréquence d'analyse

Suite à cela, une fenêtre où vous pourrez sélectionner le type d'analyse s'affichera. Cochez la case **Une seule fois** si vous voulez programmer une analyse ponctuelle. Si vous souhaitez que l'analyse soit répétée après un certain intervalle, cochez la case **Périodiquement**.

Figure 27

Tapez dans le champ **Tous les** le nombre de minutes / heures / jours / semaines / mois / années après lequel vous voulez répéter ce processus.

Vous pouvez cliquer sur les flèches de cette boîte afin d'augmenter / baisser le nombre de minutes / heures / jours / semaines / mois / années.

Sélectionnez l'intervalle - minutes, heures, jours, semaines, mois, années – après lequel l'analyse sera répétée. Faîtes défiler la liste et choisissez l'unité de temps souhaitée.

Si vous choisissez une analyse répétée, l'évènement sera lancé pour une période de temps illimitée. Afin de le stopper, il doit être effacé de la liste des évènements de la fenêtre du **Planificateur**.

Après avoir sélectionné la période, cliquez sur **Suivant** pour continuer. Si vous souhaitez revenir en arrière, cliquez sur **Précédent**.

3. Selection des objets à analyser

Cette étape permet de sélectionner les objets que vous souhaitez analyser – le secteur de boot, les fichiers, les archives, les fichiers en paquets.

Figure 28

Sélectionnez un ou plusieurs objets à analyser, en cochant simplement ceux que vous souhaitez.

Vous pouvez sélectionner les objets suivants:

- Boot – pour analyser le secteur de boot, afin d'identifier les virus de boot;
- **Fichiers** – pour analyser les fichiers;
- **Archive messagerie** – pour analyser les archives de mail;
- Archives – pour analyser à l'intérieur des archives;
- Paquets – pour analyser les fichiers en paquets.

Cliquez sur **Suivant**.

4. Sélection du chemin

Ici vous devez spécifier le répertoire des objets à analyser, comme observé sur la capture. Cette étape est nécessaire si vous avez sélectionné l'analyse de fichiers dans l'étape précédente.

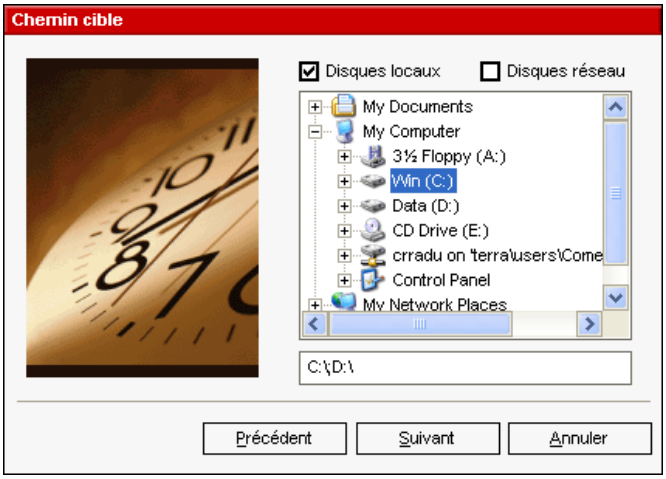


Figure 29

Cet écran est une fenêtre d'exploration qui vous permet de sélectionner les partitions et répertoires à analyser.

Lorsque le curseur est placé sur un répertoire, le chemin complet du répertoire apparaîtra dans le champ inférieur.

Cliquez sur la case "+" pour ouvrir une option ou sur celle "-" pour fermer une option.

Par ailleurs, pour sélectionner les éléments à analyser, vous pouvez utiliser les options de sélection rapide placées en haut de la fenêtre:

- **Disques locaux** - pour analyser tous les disques locaux;
- **Disques réseau** - pour analyser tous les disques du réseau.

Cliquez sur **Suivant**.

5. Sélection des types de fichiers

Spécifiez les types e fichiers à analyser.

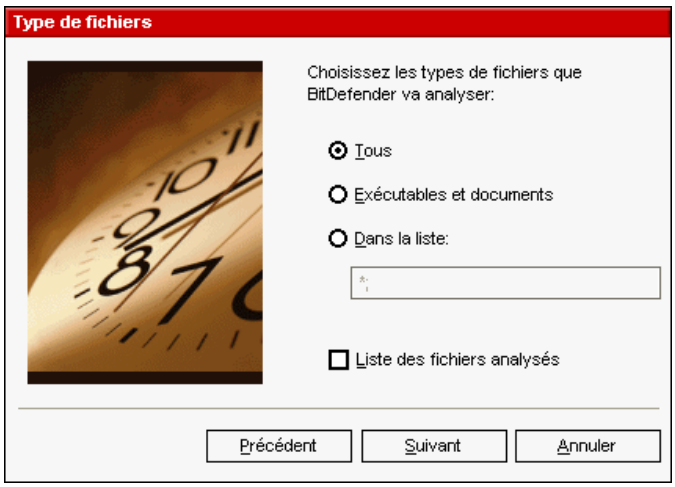


Figure 30

Cette étape est nécessaire seulement si vous avez sélectionné l'analyse de fichiers.

Vous pouvez sélectionner:

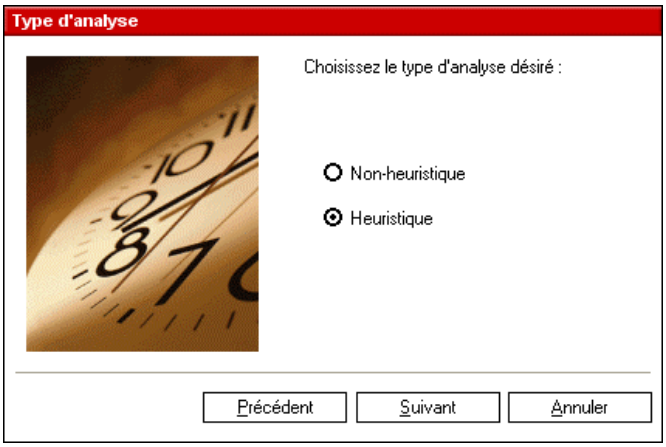
- **Tous** – pour analyser tous les fichiers, quel que soit leur type;
- **Exécutables et documents** – pour analyser les fichiers programmes et les documents;
- **Dans la liste** – pour analyser seulement les fichiers dont l'extension apparaît dans la liste. Ces extensions doivent être séparées par ";".

Si vous souhaitez voir les informations sur l'ensemble des fichiers scannés, infectés ou non, sélectionnez l'option **Liste des fichiers analysés**.

Cliquez sur **Suivant**.

6. Sélection du type d'analyse

Sélectionnez le type d'analyse.



Cela, comme indiqué sur l'image, permet de sélectionner l'un des deux types d'analyse:

Figure 31

- **Analyse** Non-heuristique - analyse les fichiers avec une procédure basée sur des signatures de virus connus. Pour activer ce type d'analyse, sélectionnez **Non-Heuristique**;
- **Analyse** Heuristique – représente une méthode basée sur certains algorithmes, qui permettent d'identifier de nouveaux virus encore inconnus. Parfois, elle peut générer des rapports de codes suspects dans des programmes normaux, ce que l'on appelle des "false positive" (ou fausse alerte). Pour activer ce type d'analyse, sélectionnez **Heuristique**.

Cliquez sur **Suivant**.

7. Selection de l'action sur les fichiers infectés

BitDefender permet de choisir deux actions dans le cas où des fichiers infectés sont trouvés.

Nous vous recommandons de sélectionner **Désinfecter** en première action et **Déplacer en Quarantaine** en seconde action.

Figure 32

Vous pouvez sélectionner l'une des actions suivantes pour la première action:

Action	Description
Désinfecter	Pour désinfecter les fichiers infectés.
Effacer	Pour supprimer les fichiers infectés. Cette action n'est pas recommandée!
Déplacer en quarantaine	Les fichiers infectés sont déplacés en quarantaine. Lorsque le virus est en quarantaine il ne peut avoir aucune action néfaste.
Renommer	Pour changer l'extension des fichiers infectés. La nouvelle extension des fichiers infectés sera `.vir`. En renommant les fichiers infectés, la possibilité d'exécuter et donc de propager l'infection disparaît. En même temps, ils peuvent être sauvegardés pour un examen et analyse ultérieur.
Demander	Chaque fois qu'un fichier infecté est détecté, une boîte de dialogue est affichée, dans laquelle l'utilisateur peut sélectionner l'action à entreprendre sur ce fichier. Il est recommandé de choisir l'action suivant l'importance du fichier.
Ignorer	Dans ce cas, l'infection est ignorée et aucune action n'est réalisée sur le fichier infecté. Seul son statut sera rapporté.

Sélectionnez la seconde action à prendre sur les fichiers infectés:

Action	Description
Effacer	Supprimer les fichiers infectés automatiquement, sans aucune alerte.
Déplacer en quarantaine	Les fichiers infectés sont déplacés en quarantaine. Lorsque le virus est en quarantaine il ne peut avoir aucune action néfaste.
Renommer	Pour changer l'extension des fichiers infectés. La nouvelle extension des fichiers infectés sera `.vir`. En renommant les fichiers infectés, la possibilité d'exécuter et donc de propager l'infection disparaît. En même temps, ils peuvent être sauvegardés pour un examen et analyse ultérieur.
Demander	Chaque fois qu'un fichier infecté est détecté, une boîte de dialogue est affichée, dans laquelle l'utilisateur peut sélectionner l'action à entreprendre sur ce fichier. Il est recommandé de choisir l'action suivant l'importance du fichier.
Ignorer	Dans ce cas, l'infection est ignorée et aucune action n'est réalisée sur le fichier infecté. Seul son statut sera rapporté.

Cliquez sur **Suivant**.

8. Création du rapport

Choisissez comment créer un fichier de rapport d'analyse.

Figure 33

Pour créer un rapport d'analyse, cliquez sur **Créer fichier rapport**. Dès lors, les autres options pour la création d'un fichier rapport seront activées.

Tapez le nom du fichier rapport dans la case **Nom du rapport**. Par défaut, le nom est `schedule.log`. Il contiendra toutes les informations concernant le processus d'analyse : le nombre de virus identifiés, le nombre de fichiers analysés, le nombre de fichiers désinfectés et supprimés.

Cliquez sur **Ajouter** si vous souhaitez ajouter à un fichier rapport existant les informations d'une nouvelle analyse, construisant ainsi un mini historique des résultats des analyses réalisées à différents moments.

Cliquez sur **Remplacer** si vous souhaitez créer un nouveau fichier rapport à chaque nouvelle analyse lancée. Dans ce cas, les informations concernant la précédente analyse seront effacées.

Astuce: Vous pouvez voir le fichier rapport dans la section Rapport du module **Antivirus**.

Cliquez sur **Suivant**.

9. Consulter les propriétés de la tâche

Il s'agit de la dernière étape dans la création d'une tâche d'analyse.

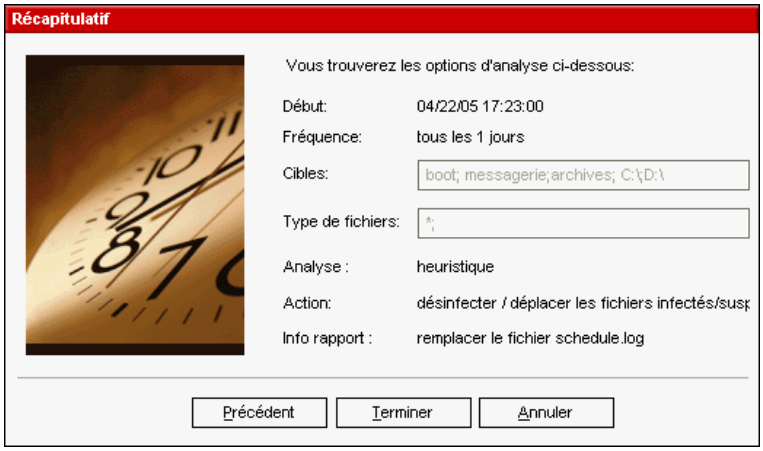


Figure 34

Dans cette fenêtre vous pouvez, voir tous les paramétrages de la tâche d'analyse et vous pouvez les modifier en retournant sur les étapes précédentes (**Précédent**). Si vous ne souhaitez faire aucune modifications, cliquez sur **Terminer**.

La nouvelle tâche apparaîtra dans la section **Planificateur**.

Pour chaque tâche d'analyse programmée, vous pouvez voir son nom, sa description, sa date de démarrage, la prochaine fois qu'elle sera lancée, le type de tâche (périodique ou ponctuelle), la cible, les extensions de fichiers, le type d'analyse et l'action à entreprendre sur les fichiers infectés.

Note

Lors de la modification d'une tâche d'analyse, les mêmes étapes seront suivies. Dans le cas d'une modification du nom de l'évènement, une nouvelle tâche sera créée. Par exemple, si nous avons l'évènement EV1 et que nous avons modifié son nom en EV2, EV1 ne disparaîtra pas, à l'inverse une nouvelle tâche nommée EV2 avec les mêmes propriétés que EV1 apparaîtra.

Si vous faites un clic-droit sur une tâche programmée, un menu s'affichera comme celui ci-dessous:

Figure 35

Si aucun évènement n'est sélectionné, et que vous faites un clic-droit sur la section **Planificateur**, seule l'option Créér sera active, toutes les autres seront inaccessibles.

Astuce: Le **Planificateur** permet un nombre illimité de tâches d'analyse.

Vous pouvez également naviguer à travers les tâches d'analyse en utilisant le clavier : appuyer sur la touche **Delete** pour effacer une tâche, pressez la touche **Enter** afin de voir les propriétés de l'événement sélectionné ou appuyez sur la touche **Insert** pour créer une nouvelle tâche (l'assistant du **Planificateur** se lancera).

Utilisez les touches de navigation pour faire défiler la page de bas en haut et de gauche à droite.

Isoler les fichiers infectés

BitDefender permet d'isoler les fichiers infectés ou suspects dans une zone sécurisée, nommée quarantaine. En isolant ces fichiers dans la quarantaine, le risque d'être infecté disparaît et, en même temps, vous avez la possibilité d'envoyer ces fichiers pour une analyse par le VirusLab de BitDefender. La section qui permet d'administrer ces fichiers isolés est la **Quarantaine**. Ce module a été conçu avec une fonction d'envoi automatique des fichiers infectés au VirusLab.

Dans le cas où vous n'auriez pas encore ouvert la console de management, vous pouvez y accéder depuis le menu Démarrer de Windows en suivant le chemin suivant **Démarrer** → **Programmes** → **BitDefender** → **BitDefender 8 Standard** ou plus rapidement en double-cliquant sur l'icône BitDefender dans la zone de notification.

Dans la console de management, cliquez sur le module **Antivirus** puis sur l'onglet **Quarantaine**.

BitDefender 8 Standard
Résident
Analyse
Planificateur
Quarantaine
Rapport
Général
Antivirus
Mise à jour
Nom du fichier
Nom du virus
Suspect
Envoyé
dwintl.dll
Non
Non
Non
La quarantaine n'a pas de limite de taille (56 KB).
Détails
Ajouter
Effacer
Restaurer
Envoyer
Options
Quarantaine
La Quarantaine garde les fichiers suspects pour être analysés. Pendant la période durant laquelle un fichier se trouve en Quarantaine, il ne peut pas être exécuté. Par défaut, les fichiers suspects sont soumis au laboratoire BitDefender. Vous pouvez cependant choisir de ne pas les envoyer. Afin de copier un fichier suspect dans la Quarantaine, cliquez sur le bouton [Ajouter] ou simplement glissez-déposez-le dans la Quarantaine, cliquez sur le bouton [Restaurer] pour le faire sortir de la Quarantaine, et le remettre dans son emplacement d'origine.
Plus d'infos

Figure 36

Comme vous le constaterez, la section **Quarantaine** contient une liste de tous les fichiers qui ont été isolés jusque là. Chaque fichier intègre son nom, sa taille, sa date d'isolation et sa date de soumission. Si vous voulez voir plus d'informations à propos des fichiers en quarantaine, cliquez sur **Plus d'infos**.

Note
Lorsque le virus est en quarantaine, il ne peut faire aucun dégât puisqu'il ne peut être exécuté ou lu.

La section **Quarantaine** contient des boutons pour administrer ces fichiers:

- **Ajouter** – ajoute des fichiers à la quarantaine. Utilisez ce bouton pour mettre en quarantaine un fichier que vous soupçonner d'être infecté. Une fenêtre s'ouvrira et vous pourrez sélectionner le fichier depuis son emplacement sur le disque. De cette façon, le fichier est copié en quarantaine. Si vous voulez déplacer le fichier en zone de quarantaine, vous devez cocher la case **Supprimer de l'emplacement d'origine**. Une méthode plus rapide d'ajouter des fichiers suspects à la quarantaine est de les glisser – déposer dans la liste de quarantaine.
- **Supprimer** – supprime les fichiers sélectionnés de votre ordinateur.

➔ **Restaurer** – remet le fichier sélectionner à son emplacement d'origine.
➔ **Envoyer** – envoie les fichiers sélectionnés pour analyse au VirusLab. Vous devez spécifier quelques informations pour pouvoir les soumettre. Pour cela, cliquez sur **Paramétrages** et complétez les champs de la section **Paramétrages Emails**, comme décrit ci-dessous.

Note
Par défaut, les fichiers suspects sont soumis pour analyse au VirusLab. Cependant vous pouvez choisir de ne pas les soumettre en désélectionnant l'option **Envoyer automatiquement la quarantaine** depuis les paramétrages de la quarantaine.

➔ **Options** – ouvre les options avancées pour la zone de quarantaine. La fenêtre suivante s'ouvrira:

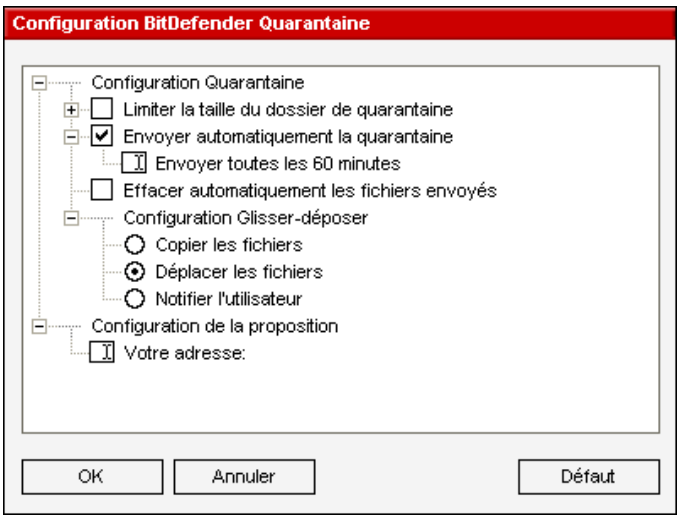


Figure 37

Les options de quarantaine sont groupées en deux catégories:

- **Configuration quarantaine**
- **Configuration de la proposition**

Cliquez sur la case avec un "+" pour ouvrir une option ou la boîte avec un "-" pour fermer une option.

Configuration Quarantaine

➔ **Limiter la taille du dossier de quarantaine** - maintient sous contrôle la taille de la quarantaine. Cette option est activée par défaut et sa taille est de 12 000 kbs. Si vous voulez changer cette valeur, vous pouvez en introduire une autre dans le champ **La taille maximale du dossier de quarantaine est**.

L'option **Effacer automatiquement les vieux fichiers** est utilisée pour supprimer les anciens fichiers lorsque la quarantaine est pleine et qu'il n'y a plus de place pour ajouter de nouveaux fichiers.

➔ **Envoyer automatiquement la quarantaine** – envoie automatiquement les fichiers en quarantaine au VirusLab pour analyse. Vous pouvez paramétrer le délai entre deux envois consécutifs dans le champs **Envoyer toutes les**.
➔ **Effacer automatiquement les fichiers envoyés** – supprime automatiquement les fichiers en quarantaine après les avoir envoyés au VirusLab pour analyse.
➔ **Configuration Glisser – déposer** – si vous utilisez la méthode du glisser - déposer pour ajouter de nouveaux fichiers à la quarantaine, vous pouvez ici spécifier l'action : copier, déplacer ou demander à l'utilisateur.

Configuration de la proposition

Vous devez spécifier votre adresse e-mail afin d'envoyer des fichiers en quarantaine au VirusLab.

➔ **Votre adresse** – entrez votre adresse e-mail dans le cas où vous souhaitez recevoir une réponse de nos experts au sujet des fichiers suspects soumis pour analyse.

Afficher les fichiers rapports

Lors du lancement d'un processus d'analyse, l'utilisateur a la possibilité d'opter pour la création d'un fichier rapport où il peut voir des informations au sujet de l'analyse. L'utilisateur peut voir ces rapports depuis la console de management.

Dans le cas où vous n'auriez pas encore ouvert la console de management, vous pouvez y accéder depuis le menu Démarrer de Windows en suivant le chemin suivant **Démarrer → Programmes → BitDefender → BitDefender 8 Standard** ou plus rapidement en double-cliquant sur l'icône BitDefender dans la zone de notification.

Dans la console de management, entrez dans le module **Antivirus** et cliquez sur l'onglet **Rapports**.

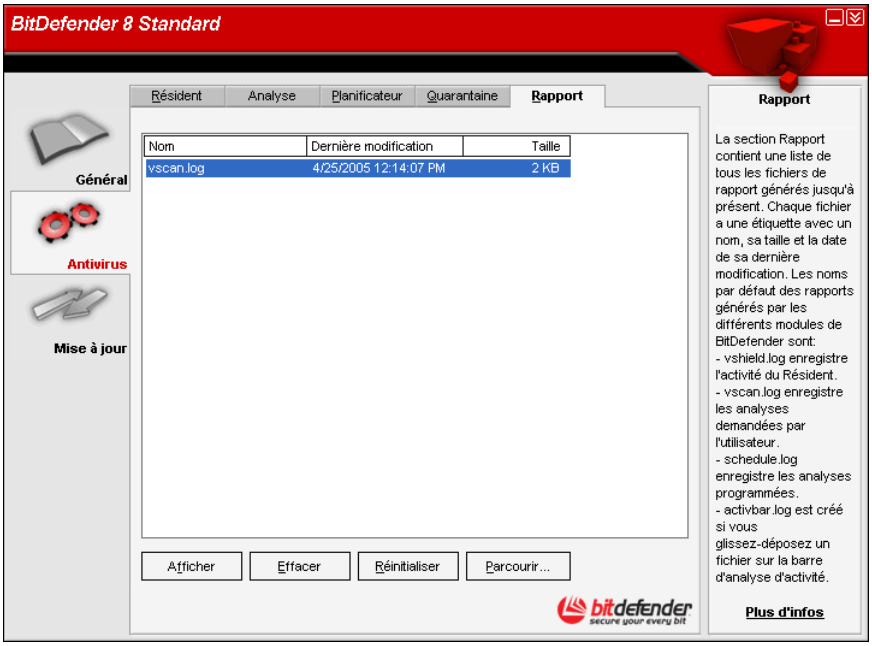

BitDefender 8 Standard
Général
Antivirus
Mise à jour
Résident
Analyse
Planificateur
Quarantaine
Rapport
Nom
Dernière modification
Taille
vscan.log
4/25/2005 12:14:07 PM
2 KB
Afficher
Effacer
Réinitialiser
Parcourir...
Rapport
La section Rapport contient une liste de tous les fichiers de rapport générés jusqu'à présent. Chaque fichier a une étiquette avec un nom, sa taille et la date de sa dernière modification. Les noms par défaut des rapports générés par les différents modules de BitDefender sont:
- vshield.log enregistre l'activité du Résident.
- vscan.log enregistre les analyses demandées par l'utilisateur.
- schedule.log enregistre les analyses programmées.
- activbar.log est créé si vous glissez-déposez un fichier sur la barre d'analyse d'activité.
Plus d'infos

Figure 38

BitDefender conservera des traces de sa propre activité sur votre ordinateur. Les fichiers rapports par défaut sont les suivants:

- Vshield.log est l'historique que BitDefender écrit lors de son analyse permanente de vos emails, téléchargements et programmes actifs ou fichiers à l'accès sur votre système;
- Vscan.log est créé lorsque vous scannez immédiatement votre système;
- Schedule.log vient des tâches d'analyse que vous pouvez avoir paramétré;
- Activbar.log est créé lorsque vous analysez par la fonction glisser & déposer.

La section **Rapport** contient une liste de tous les fichiers rapports générés. Chaque fichier a son nom, sa taille et sa date de dernière modification. Il y a des boutons créés pour l'administration de ces fichiers rapports.

La fonction de chacun de ces boutons est expliquée ci-après:

➔ **Afficher** – ouvre le fichier rapport sélectionné.
➔ **Effacer** – supprime le fichier rapport sélectionné.

- ➔ **Réinitialiser** – si la console de management est ouverte à la section **Rapport** et que vous réalisez dans le même temps une analyse de votre ordinateur, le nouveau fichier rapport avec les résultats d'analyse (si vous avez sélectionné l'option **Créer un fichier rapport**) ne sera visible seulement qu'après avoir cliqué sur **Réinitialiser**.
- ➔ **Parcourir** – ouvre une fenêtre dans laquelle vous pouvez sélectionner le fichier rapport que vous souhaitez voir.

Astuce: Les fichiers rapports sont sauvegardés par défaut dans le répertoire d'installation de **BitDefender**. Si vous avez sauvegardé les fichiers rapports dans un autre répertoire, vous devez utiliser le bouton **Parcourir** pour les localiser.

Désinfection d'un virus détecté

Les virus sont beaucoup plus faciles à arrêter qu'à les désinfecter une fois entrés dans votre PC. C'est pourquoi la protection antivirus devrait être toujours active et mise à jour.

BitDefender détecte un virus résident il est recommandé d'essayer de le désinfecter. Ceci peut être impossible pour une variété de raisons, les virus résidents actifs pouvant être difficiles à gèrer.

Si **BitDefender** trouve un virus et ne peut pas le désinfecter il est recommandé de contacter notre équipe support à l'adresse sav@editions-profil.fr.

Le secret pour la désinfection d'un virus est le connaitre. Vous pouvez trouver des infos sur le virus sur notre site, http://www.bitdefender.fr.

Pour les virus les plus répandus nous vous offrons des utilitaires spéciaux de désinfection.

C'est toujours une bonne idée de chercher sur internet toute information sur le virus en question.

Contactez notre support technique à l'adresse sav@editions-profil.fr.

Module Mise à jour

De nouveaux virus sont trouvés et identifiés chaque jour. C'est pourquoi il est très important de garder BitDefender à jour avec les dernières signatures de virus. Par défaut, BitDefender recherche automatiquement des mises à jour toutes les trois heures.

Plus de fonctions

Les mises à jour se déclinent en trois parties:

- **Mise à jour produit** – lorsqu'une nouvelle version du produit est prête, de nouvelles fonctions et techniques d'analyse sont introduites afin d'augmenter les performances du produit. Ces mises à jour sont affichées sous le nom de **Product Update**;

- **Mise à jour des moteurs antivirus** – comme de nouvelles menaces apparaissent, les fichiers contenant les signatures de virus doivent être mis à jour en permanence contre elles. Elles s'affichent sous le nom de **Virus Definitions Update**.

De plus, du point de vue de l'intervention de l'utilisateur, nous proposons:

- **Mise à jour manuelle** – vérifiant l'existence d'une mise à jour à la demande de l'utilisateur;

- **Mise à jour automatique** – l'antivirus contacte automatiquement le serveur BitDefender afin de vérifier si une mise à jour est disponible. Si c'est le cas, BitDefender est actualisé automatiquement.

Si vous êtes connecté à Internet par câble ou DSL, BitDefender se charge de cela lui-même : Il recherche de nouvelles signatures de virus lorsque vous démarrez votre ordinateur puis ensuite toutes les **3 heures**. Si de nouvelles signatures de virus sont disponibles, BitDefender se met à jour lui-même.

Astuce: Si vous êtes connecté à Internet par une connexion RTC (ou Numéris), alors c'est une bonne idée que de prendre l'habitude de rechercher manuellement des mises à jour.

Mise à jour manuelle

Si vous n'avez pas encore ouvert la console de management, vous pouvez y accéder depuis le menu Démarrer de Windows, en suivant le chemin **Démarrer** → **Programmes** → **BitDefender 8** → **BitDefender 8 Standard** ou plus rapidement en double-cliquant sur l'icône BitDefender dans la zone de notification.

Dans la console de management, cliquez sur **Mise à jour**.

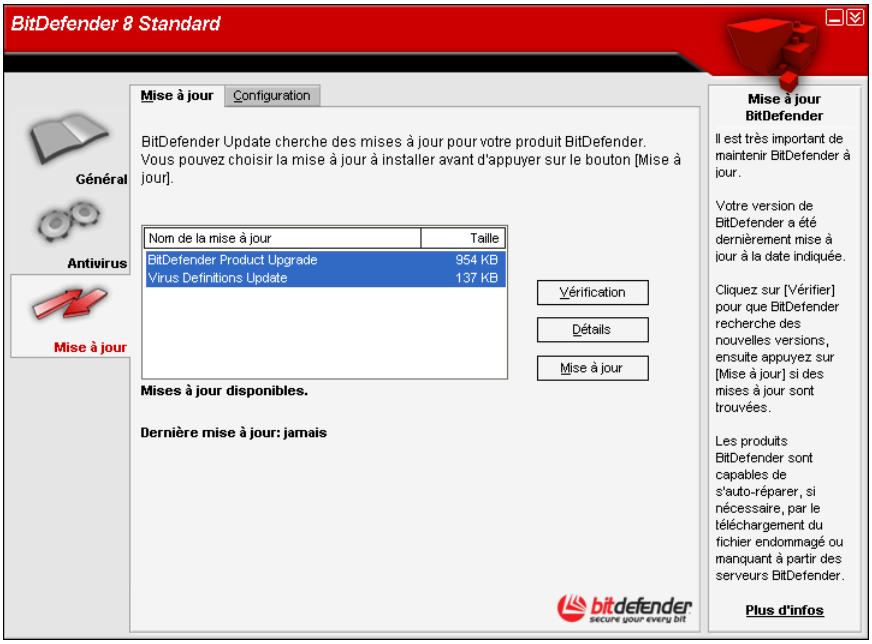

BitDefender 8 Standard
Mise à jour
Configuration
Général
Antivirus
Mise à jour
BitDefender Update cherche des mises à jour pour votre produit BitDefender. Vous pouvez choisir la mise à jour à installer avant d'appuyer sur le bouton [Mise à jour].
Nom de la mise à jour
Taille
BitDefender Product Upgrade
954 KB
Virus Definitions Update
137 KB
Vérification
Détails
Mise à jour
Mises à jour disponibles.
Dernière mise à jour: jamais
Mise à jour BitDefender
Il est très important de maintenir BitDefender à jour.
Votre version de BitDefender a été dernièrement mise à jour à la date indiquée.
Cliquez sur [Vérifier] pour que BitDefender recherche des nouvelles versions, ensuite appuyez sur [Mise à jour] si des mises à jour sont trouvées.
Les produits BitDefender sont capables de s'auto-réparer, si nécessaire, par le téléchargement du fichier endommagé ou manquant à partir des serveurs BitDefender.
Plus d'infos

Figure 39

La mise à jour manuelle peut être lancée à tout moment, même si le produit était configuré en mise à jour automatique. Pour mettre à jour manuellement le produit, suivez ces étapes:

- Cliquez sur **Vérification**. Le module **Mise à jour** se connectera au serveur BitDefender et vérifiera la disponibilité d'une mise à jour.
- Si une mise à jour est détectée, son nom et sa taille seront affichés. Cliquez sur **Mise à jour** pour démarrer le processus de mise à jour.

Astuce: Si vous souhaitez voir quels fichiers seront mis à jour, cliquez sur **Détails**.

Si aucune mise à jour n'est détectée le message suivant apparaîtra **Aucune mise à jour disponible!**.

Note

Il peut être nécessaire de redémarrer votre PC lorsque vous avez terminé une mise à jour. Nous vous recommandons de le faire dès que possible.

Mise à jour automatique

Si vous êtes un utilisateur avancé, cliquez sur l'onglet **Configuration** afin de configurer le module **Mise à jour**.

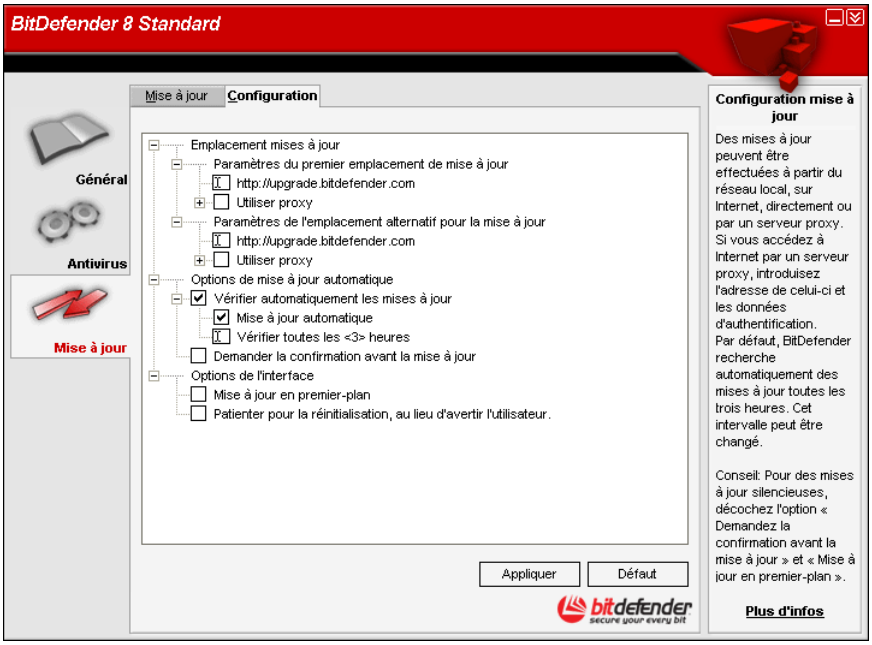

BitDefender 8 Standard
Mise à jour
Configuration
Général
Antivirus
Mise à jour
Emplacement mises à jour
Paramètres du premier emplacement de mise à jour
http://upgrade.bitdefender.com
Utiliser proxy
Paramètres de l'emplacement alternatif pour la mise à jour
http://upgrade.bitdefender.com
Utiliser proxy
Options de mise à jour automatique
Vérifier automatiquement les mises à jour
Mise à jour automatique
Vérifier toutes les <3> heures
Demander la confirmation avant la mise à jour
Options de l'interface
Mise à jour en premier-plan
Patienter pour la réinitialisation, au lieu d'avertir l'utilisateur.
Appliquer
Défaut
bitdefender
Configuration mise à jour
Des mises à jour peuvent être effectuées à partir du réseau local, sur Internet, directement ou par un serveur proxy. Si vous accédez à Internet par un serveur proxy, introduisez l'adresse de celui-ci et les données d'authentification. Par défaut, BitDefender recherche automatiquement des mises à jour toutes les trois heures. Cet intervalle peut être changé.
Conseil: Pour des mises à jour silencieuses, décochez l'option « Demandez la confirmation avant la mise à jour » et « Mise à jour en premier-plan ».
Plus d'infos

Figure 40

Les mises à jour peuvent être réalisées depuis le réseau local, depuis Internet, directement ou à travers un serveur proxy.

La fenêtre avec les paramétrages de mises à jour contient trois catégories d'options (**Emplacement mises à jour, Options de mise à jour automatique, Options de l'interface**) organisées en menus extensibles, similaires à ceux de Windows.

Cliquez sur la case "+" pour ouvrir une option ou sur celle "-" pour fermer une option.

Emplacement mises à jour

Pour des mises à jour plus rapides et plus fiables, vous pouvez établir deux locations de mise à jour : une **Location Principale de mise à jour** et une **Location Alternative de mise à jour**. Pour les deux, vous devez établir les options suivantes:

➔ Si vous êtes connectés à un réseau local sur lequel sont placées les signatures de virus de BitDefender, vous pouvez changer l'emplacement des mises à jour ici. Par défaut, c'est le suivant: http://upgrade.bitdefender.com.

➔ **Utilisez proxy** – Dans le cas où la société utilise un serveur proxy, cochez cette option. Les paramétrages suivants doivent être spécifiés.

- **Serveur proxy** – tapez l'IP ou le nom du serveur proxy et le port que BitDefender doit utiliser pour se connecter au serveur proxy.

  Syntaxe: `name:port` ou `ip:port`.

- **Utilisateur** – tapez ici un nom d'utilisateur reconnu par le proxy.

Syntaxe: `domain\user`.

- **Mot de passe** – tapez ici un mot de passe valide pour l'utilisateur précédemment spécifié.

Options de mise à jour automatique

➔ **Vérifier automatiquement les mises à jour** – Cela assure que BitDefender contrôle automatiquement nos serveurs pour la disponibilité de mises à jour.

- **Mise à jour automatique** – Si BitDefender détecte une nouvelle mise à jour sur nos serveurs, alors avec cette option cochée, BitDefender télécharge et implémente la mise à jour.

- **Vérifier toutes les <x> heures** – Paramétrez la fréquence de recherche de mise à jour de BitDefender. L'intervalle de temps par défaut est de 3 heures.

➔ Gardez sélectionné **Demander confirmation avant mise à jour** si vous souhaitez être interrogé avant le téléchargement et l'installation des mises à jour.

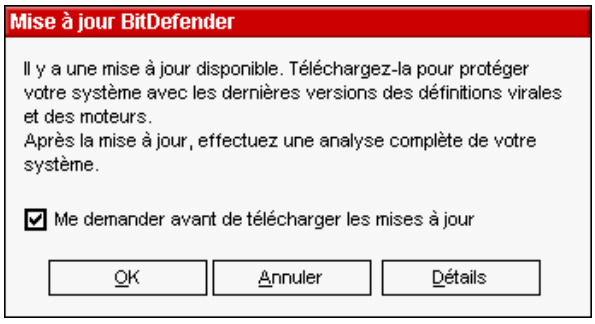

Mise à jour BitDefender
Il y a une mise à jour disponible. Téléchargez-la pour protéger votre système avec les dernières versions des définitions virales et des moteurs.
Après la mise à jour, effectuez une analyse complète de votre système.
Me demander avant de télécharger les mises à jour
OK
Annuler
Détails

Figure 41

Cliquez sur **OK** pour démarrer le processus de mise à jour, cliquez sur **Détails** pour voir quels fichiers seront actualisés ou cliquez sur **Annuler** pour mettre à jour plus tard.

Options de l'interface

➔ **Mise à jour en premier plan** – Par défaut la mise à jour du produit se fait en arrière plan. Si vous souhaitez que la fenêtre de mise à jour soit par dessus les autres fenêtres, utilisez cette option.

➔ **Patientez pour la réinitialisation, au lieu d'avertir l'utilisateur** - Si une mise à jour nécessite la réinitialisation, le produit utilisera les fichiers anciens jusqu'à la réinitialisation du système. L'utilisateur ne sera pas averti sur la réinitialisation, c'est pourquoi le processus de mise à jour de BitDefender ne perturbera pas le travail de l'utilisateur.

Cliquez sur **Appliquer** pour enregistrer les modifications. Si vous cliquez sur **Défaut** vous allez charger les paramètres par défaut.

6

Meilleurs conseils

Antivirus

Etapes à suivre pour vous assurer un PC sans virus:

1. Après la fin de l'installation, enregistrez le produit comme décrit dans la section Enregistrement du produit.

2. Faites une mise à jour manuelle de vos signatures virales. Dans la console d'administration BitDefender, entrez dans le module Mise à jour et cliquez sur **Vérification**.

3. Faites une analyse complète de votre système (décrite dans la section Analyse immédiate de ce guide).

4. Dans la section Etat du module **Général**, laissez activées les plus importantes options de BitDefender: **Virus Shield** et **Mise à jour automatique**.

5. Programmez BitDefender à analyser votre système au moins une fois par semaine, utilisant l'assistant du Planificateur.

   Astuce: Le **Planificateur** vous laisse planifier à l'avance et programmer des analyses complètes de votre PC/disque pendant les heures quand vous n'utilisez pas le PC.

Si vous n'êtes pas la seule personne utilisant cet ordinateur, il est recommandé de protéger votre configuration BitDefender avec un mot de passe. Pour le créer, entrez dans le module **General**, section Configuration et utilisez l'option **Activer la protection par mot de passe**.

7

Questions courantes

Général

1. **Q:** Comment faire pour vérifier que BitDefender fonctionne vraiment?
   R: Dans le module **Général**, cliquez sur l'onglet Etat et regardez les statistiques.

2. **Q:** Quelles sont les demandes de système?
   R: Vous trouverez les demandes de système dans la section Installation.

3. **Q:** Comment désinstaller BitDefender?
   R: Suivez: **Démarrage → Programmes → BitDefender 8 → Modifier, réparer ou désinstaller** et dans la fenêtre qui apparaît cliquez sur **Désinstaller**. Cela démarre le processus de désinstallation.

4. **Q:** Où introduire la clef d'activation (code d'activation)?
   R: Dans le module **General**, cliquez sur l'onglet Enregistrer et cliquez sur **Introduire code d'activation**.

Antivirus

5. **Q:** Comment effectuer une analyse complète du système?
   R: Dans le module **Antivirus**, cliquez sur l'onglet Analyse, cochez **Disques locaux** et ensuite **Analyse**.

6. **Q:** Combien de fois par semaine je devrais analyser mon PC?
   R: Nous recommandons une fréquence d'au moins une fois par semaine.

7. **Q:** Comment analyser automatiquement tout fichier que je transfère dans mon PC?
   R: BitDefender analyse tous les fichiers à l'accès. Vous devez seulement maintenir Résident activé.

8. **Q:** Comment programmer BitDefender à analyser mon PC périodiquement?
   R: Dans le module **Antivirus**, cliquez sur Planificateur, sur **Nouveau** et suivez l'assistant**.**

9. **Q:** Qu'est-ce qui se passe avec les fichiers de la quarantaine?
   R: Vous pouvez les envoyer aux Laboratoires BitDefender pour analyse, mais d'abord il vous faut établir la configuration de messagerie (dans la section Quarantaine – cliquez sur **Configuration**).

Mise à jour

10. **Q:** Pourquoi est-il nécessaire de mettre à jour BitDefender?
R: Chaque fois que vous faites une mise à jour, de nouvelles signatures virales sont rajoutées aux moteurs d'analyse, et de nouvelles règles aux filtres heuristiques et URL.

11. **Q:** Comment mettre à jour BitDefender?
R: Par défaut, BitDefender se met à jour automatiquement toutes les 3 heure. Vous pouvez changer cette option ou faire la Mise à jour manuellement.

Glossaire

ActiveX	ActiveX est un modèle pour écrire des programmes tels que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour faire des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent demander ou répondre à des questions, utiliser des boutons et interagir d'autres façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic. Active X est reconnu pour un manque total de commandes de sécurité; les experts en sécurité informatique déconseillent son utilisation sur Internet.
Applete Java	Il s'agit d'un programme Java conçu pour s'exécuter seulement dans une page Web. Pour utiliser une applette dans une page Web, vous devez spécifier le nom de l'applette et la taille (la longueur et la largeur - en pixels) qu'elle peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applette depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applettes diffèrent des applications dans le fait qu'elles sont dirigées selon un protocole de sécurité strict. Par exemple, bien que les applettes s'exécutent sur le client, elles ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applettes sont également limitées pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.
Archive	(1) Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés. (2) Un fichier qui contient un ou plusieurs fichiers dans un format compressé.
Backdoor	Il s'agit d'une faille dans la sécurité d'un système délibérément laissé en place par des développeurs ou mainteneurs. La motivation n'est pas toujours négative; quelques logiciels permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.
Chemin	1. Les directions exactes vers un fichier. Ces directions sont décrites d'habitude par arborescence, de haut en bas, comportant le disque, dossier, sous-dossier, fichier, extension du fichier: c:\jobscompany\note.txt. Ce kit d'informations est un chemin complet. 2. La connexion entre deux points, telle le canal de communication entre deux ordinateurs.
Client de messagerie	Un client de messagerie est un logiciel qui vous permet d'envoyer et recevoir des messages (e-mails).

Cookie	Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une épée à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent (vous voyez seulement des annonces vous intéressant) mais d'autre part, cela implique en réalité "le pistage" et "le suivi" d'où vous allez et de ce sur quoi vous cliquez sur Internet. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple " numéro SKU " (vous savez, le code barres à l'arrière des produits). Bien que ce point de vue puisse paraître extrême, dans certains cas cette perception est justifiée.
Définition virus	La "signature" binaire du virus, utilisé par l'antivirus pour la détection et l'élimination du virus.
Disk drive	C'est une appareil qui lit et écrit des données sur un disque. Une **unité de disque dur** lit et écrit sur un disque dur. Un **lecteur de disquette** accède à des disquettes. Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).
Evénements	Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme l'analyse de la mémoire. Le Scheduler est un outil qui vous aide à programmer vos tâches d'analyse.
Extension de fichier	La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier. De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS Dos. Elles comportent communément une à trois lettres (certains vieux OS ne supportent pas plus de trois). Exemples: "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.
Fausse alerte	Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.
Fichier journal	Un fichier qui enregistre les actions qui surviennent. Par exemple, BitDefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.
Heuristique	Méthode permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter des variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

IP	**Protocole Internet** - Un protocole routable de la suite de protocoles TCP/IP qui se charge de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.
Ligne de commande	Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.
Mémoire	Zone de stockage interne dans votre ordinateur. Le terme *mémoire* regarde le stockage des données dans les "chips" (composants), et le terme *stockage* regarde les disques. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.
Messagerie électronique	Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.
Mise à jour	Une nouvelle version du logiciel ou d'un produit hardware, destinée à remplacer une ancienne version du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, sinon la mise à jour ne se fait pas. BitDefender comporte un module spécial pour la mise à jour. Ce module vous permet de chercher manuellement les mises à jour ou de faire la mise à jour automatiquement.
Navigateur	Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les deux navigateurs les plus populaires sont Netscape Navigator et Microsoft Internet Explorer. Les deux sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugins) pour certains formats.
Non-heuristique	Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut paraître un virus et ne génère donc pas de fausses alertes.
Objets menu démarrage	Tous les fichiers placés dans ce dossier s'ouvrent au démarrage. Par exemple, un écran de démarrage, un fichier son pour quand l'ordinateur démarre, un calendrier, des programmes, peuvent être placées dans ce dossier. D'habitude c'est un raccourci vers le fichier qui est mis dans le dossier, et pas le fichier.
Port	(1) Une interface de l'ordinateur à laquelle vous pouvez connecter un périphérique. Les PCs comportent plusieurs sortes de ports. A l'intérieur, quelques ports pour la connexion des disques, cartes vidéo, ... A l'extérieur, les PCs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques. (2) Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Programmes empaquetés	Un fichier comprimé. Beaucoup de plates-formes et applications contiennent des commandes vous permettant de comprimer un fichier pour qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide". Normalement, cela nécessite 10 octets. Pourtant, un logiciel qui comprime les fichiers remplace la série d'espaces par un caractère spécial série d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.
Script	Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.
Secteur de boot	Un secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge la plate-forme.
System tray	Introduit avec Windows 95, le system tray se situe dans la barre de tâches Windows (à côté de l'horloge) et contient des icônes miniatures pour des accès faciles aux fonctions système: fax, imprimante, modem, volume etc. Double cliquez ou clic droit sur une icône pour voir les options.
Téléchargement	Copier des données (généralement un fichier entier) d'une source principale à un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.
TCP/IP	Transmission Control Protocol/Internet Protocol - Un ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés avec divers architectures hardware et diverses plates-formes. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.
Trojan	Un programme destructif qui prétend être une application normale. Les Trojans ne sont pas des virus et ne se repliquent pas, mais peuvent être tout aussi destructifs. Un des types les plus répandu de Trojans est un logiciel prétendant désinfecter votre PC (mais au lieu de faire cela il l'infecte). Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Trojans, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.
Ver Internet	Un programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure qu'il se propage. Il ne peut pas s'attacher aux autres programmes.
Virus	Un programme ou morceau de code qui est chargé dans votre ordinateur sans que vous le sachiez et fonctionne contre votre gré. La plupart des virus peuvent se répliquer. Tous les virus sont

	crées par des personnes. Un virus simple peut faire une copie de lui-même très vite et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est capable de se transmettre via un réseau par exemple.
Virus de boot	Un virus qui infecte le secteur de boot d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus de boot rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.
Virus macro	Un type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent des langages macro. Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.
Virus polymorphique	Un virus qui change de forme avec chaque fichier qu'il infecte. Comme ils n'ont pas une forme unique bien définie, ces virus sont plus difficiles à identifier.

Informations contact

LE SUPPORT TECHNIQUE:

SOFTWIN et Editions Profil s'efforcent de fournir à ses clients des réponses rapides et précises à vos questions. Le Centre de Support, dont vous pouvez consulter les coordonnées ci-dessous, est actualisé en continu et vous donne accès aux toutes dernières descriptions des virus et aux questions les plus fréquemment posées afin de vous répondre en temps utile.

Support technique:

- Par Email: sav.bitdefender@editions-profil.fr
- Par Chat on-line 24h/24 - 7j/7: www.bitdefender.com
- Par courrier: Editions Profil - 49 rue de la Vanne - 92120 Montrouge

Contacts Commercial et Administratif:

commercial@editions-profil.fr

BitDefender 8 Standard
Copyright 2004 SOFTWIN / ROMANIA

SOFTWIN
Str. Fabrica de Glucoza, Nr.5
Bucuresti, Sector 2, CP 52-93
ROMANIA
0040-21-233 07 80

www.bitdefender.fr

Le support technique téléphonique n'est pas accessible aux personnes disposant d'une version shareware de BitDefender ou d'une version livrée en standard avec un ordinateur (OEM).